Introducing **IPENDO®**

**IPENDO®** is an Intellectual Property Management Software (IPMS) for corporates and enables the IP team to securely connect all aspects of IP related activity, from inventor disclosure or trademark requests through to large-scale renewals payments.

To read more about the product features, please visit www.cpaglobal.com.

**Datacenter Security**

**IPENDO®,** is hosted on CPA Global owned and managed virtualised infrastructure running on a hardware stack co-located within Rackspace datacenters in the US and EU as a multi-tenant private cloud hosted SaaS product. The datacenter is housed in non-descript facility and have extensive security provisions with perimeter control utilizing professional security staff, video surveillance, intrusion detection and other electronic means. Authorized staff must pass two-factor authentication to access datacentre floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

All datacenters are Tier-3 compliant, SSAE16 & ISO27001 certified, have 24x7 surveillance, monitoring, electronic and biometric access controls, visitor management, multi-tier power backup, fire detection and suppression systems and climate controls. The datacenters have network service provider and path diversity for Internet or point-to-point network circuits.

To read further on Rackspace Datacenter Security please read https://www.rackspace.com/about/datacenters

**Co-Lo Hosting Locations for IPENDO®**

<table>
<thead>
<tr>
<th>North America (US)</th>
<th>Ashburn, VA, USA. Service Provider - Rackspace</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (EU)</td>
<td>London, UK. Service Provider - Rackspace</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Certifications / Attestations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC:ISO27001</td>
</tr>
<tr>
<td>AICPA SOC2 Type 2</td>
</tr>
</tbody>
</table>

**Security Features**

**IPENDO®** is a multi-tenant SaaS product and hosted on co-located datacenters in the US and EU. The production environment is built for fault tolerance on virtualised infrastructure using high servers and Storage Area Network (SAN) over gigabit network equipment’s. The networks and hardware infrastructure are monitored 24x7 by Rackspace as a managed service allowing CPA Global DevOps team to focus on product availability, security, issue management, deployment automations, conduct backups and recovery and streamline operations.

**Host Security**

All hosts run on security hardened Microsoft Server and undergo regular patching cycles. The hosts also installed with Anti-Virus, Anti-Malware, Local Firewall solutions.

**Environment Segregation**

Production and Development/QA environments are segregated in separate instances both on application and Database level. Each client instance runs in a separate database for complete isolation between different clients.

Additionally, procedures are in place to ensure production data is not used in nonproduction environments, unless approved by clients.
### Data Segregation

IPENDO® is a SaaS product and the customers data are segregated on Database level and all clients have their own database.

### Network Security

All production instances and non-production environments are secured through a multi-layered security topology with Layer 3 firewall, Load Balancers, Intrusion Prevention and Denial of Service (DoS) protection. Traffic flow policies are enforced through ACLs on each managed interface. Any changes to network rules or configuration are subject to a formal change approval from security team. The load balancers are also configured to support end-to-end traffic encryption using Transport Layer Security (TLS).

IPENDO® can be configured for IP Whitelisting to restrict access from client provided IP network ranges only.

### User Access Management

IPENDO® has password policy configuration and supports two factor authentication using onetime password tokens. Each client administrator can configure role-based and context-based entitlements while granting access to tenant data.

Clients are responsible for keeping passwords from being disclosed to unauthorized parties and for choosing passwords with sufficient entropy as to be effectively non-guessable.

### Privileged Access Management

The Information Security Policy at CPA Global requires that access to information assets to be granted based on business justification, with the appropriate authorization and limited based on "need-to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews.

All controls are implemented for segregation of duties, role-based access and access to resources is granted on the principle of least privilege. Logging and monitoring of privileged access to information security management systems is enforced in accordance with CPA Global Log Management and Monitoring Policy, reviewed on regular basis.

### Encryption & Key Management

Industry-standard encryption protocols and ciphers are used to enable encryption for data in transit. TLS v1.1 and higher is implemented with key exchange algorithm that supports perfect forward secrecy and provides encryption of 128 bits or stronger.

CPA Global has policies, procedures, and mechanisms established for effective key management to support encryption of data in storage and in transmission, including requisition, key generation, transmission, storage, access, rotation, renewal and revocation.

### Capacity Management

Proactive monitoring across the full stack continuously measures the performance of key subsystems of the product against the established boundaries for acceptable service performance and availability. Upon breach of any thresholds or an irregular event occurs, the monitoring system generates warnings so that operations staff can address the threshold or event. System performance and capacity utilization is proactively planned to optimize the environment.

The networks and virtualized hardware infrastructure is monitored 24x7 by Rackspace as a managed service to identify and resolve any capacity issues proactively.

### Resilience and Recovery

IPENDO® leverages the storage level backup and replication capabilities. In the event of a disaster scenario, servers are provisioned, and the recovery process is initiated using the recent backups of the systems.
Disaster Recovery test is conducted annually, and a real-time simulation test would include the following steps:

Phase 1: Disaster Recovery Launch Authorization phase - to detect service disruption or outage, determine recoverability and the extent of the damage to activate the plan.

Phase 2: Recovery phase - to break replication services, restore services and make network/URL changes.

Phase 3: Reconstitution phase - to restore processing capabilities and resume/rebuild services for primary instance.

THANK YOU