FORECAST®
Security Summary
Introducing **FORECAST®**

**FORECAST®** is an advanced, secure and easy-to-use app on *The IP Platform*, that allows you to more accurately track and predict the costs of prosecutions, filings, renewals and fees across your clients’ entire patent, trademark and design portfolio.

To read more about the product features, please visit [www.cpaglobal.com](http://www.cpaglobal.com).

**Datacenter Security**

**FORECAST®** is hosted on Amazon Web Services (AWS) provided infrastructure and platform services available in European Union (EU) as SaaS public cloud product. AWS datacenters are globally distributed, highly clustered and leverage state of the art engineering approaches to build a robust and secure hosting environment. AWS datacenters are housed in non-descript facilities and have extensive security provisions with military grade perimeter control utilizing professional security staff, video surveillance, intrusion detection and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access datacentre floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS datacenters are equipped with fire detection and suppression equipment which utilizes smoke detection sensors across the building and utility areas. The datacentre is also installed with fully redundant, serviceable 24x7 electrical power systems, UPS and generators for back-up power, climate control to ensure a consistent operating temperature for hardware, automated monitoring and management of all electrical, mechanical, life support systems and equipment.

To read further on AWS Datacenter Security please read [https://aws.amazon.com/compliance/data-center/](https://aws.amazon.com/compliance/data-center/)

<table>
<thead>
<tr>
<th>AWS Regions offered for <strong>FORECAST®</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Europe (EU)</strong></td>
<td>EU West - Ireland</td>
</tr>
</tbody>
</table>

**Certifications / Attestations**

- ISO/IEC:ISO27001
- AICPA SOC2 Type 2

**Security Features**

**FORECAST®** is a fully managed SaaS product and hosted on AWS in Europe across multiple availability zones for resilience, recovery and fault tolerance. AWS offers huge flexibility and elasticity to overall hosting and operations approach allowing to architect and dynamically scale for surges in demand. AWS allows CPA Global DevOps team to automate deployments, conduct backups and recovery instances, consume services and streamline operations, whilst allowing Self-healing (AWS Auto scaling) mechanisms to ensure maximum uptime.

**Host Security**

All hosts in AWS are deployed using application management mechanism called Elastic Beanstalk. Elastic Beanstalk auto provisions Amazon Windows Server AMI (Amazon Machine Images) to run as standardised virtual servers for seamless integration with AWS services like Elastic Block Store (EBS) for encrypted volumes, Elastic Load Balancers (ELB) coupled with Auto Scaling Groups (ASG) and CloudWatch to collect metrics and logs. Database services run on AWS Relational Database Services (RDS) AWS Aurora configured for high availability and security through encryption at rest, network isolation and assign resource-level permissions.

Virtual hosts undergo regular patching cycles and are also installed with Anti-Virus, Anti-Malware and File Integrity Monitoring.
### Environment Segregation

Production and Development/QA environments are segregated in separate AWS Virtual Private Cloud (VPC) to prevent unauthorized access or changes to information assets. AWS Identity and Access Management (IAM) is implemented to enforce clear segregation of duties for personnel accessing these environments as part of their job duties. VPC's are segregated at network level and are connected to each other through VPC-Peering (VPN equivalent). Network access is governed through Access Control Lists (ACL) on virtual firewalls. Additionally, procedures are in place to ensure production data is not used in nonproduction environments, unless approved by clients.

### Data Segregation

FORECAST® is SaaS Product and each client is logically segregated through a unique key in a shared database.

### Network Security

All production instances and non-production environments are secured through a multi-layered security topology with Layer 3 and Layer 7 firewalls, 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).

AWS environment leverages Security Groups, Subnets and Route tables in VPC to implement a complete firewall solution enabling traffic filtering by protocol, service port and source/destination IP. Traditional Layer 2 security attacks, including MAC spoofing and ARP spoofing, are blocked by default. AWS environment also has protection against Distributed Denial of Service (DDoS) through AWS Shield to prevent network and transport layer attacks.

### User Access Management

FORECAST® has password policy configuration and supports Single-Sign-On (SSO) using SAML and WS-Federated based identity federation standards through The IP Platform. Each client administrator can configure role-based and context-based entitlements while granting access to data. Clients can choose to enable Multi-Factor Authentication (MFA) on their identity store through SSO.

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.

FORECAST® has been implemented in AWS with well-defined, fine-grained roles and access into cloud hosted systems through AWS Identity and Access Management (IAM) tool. The IAM is configured to only use CPA Global’s Active Directory Federation Services (ADFS) for authenticating into AWS hosted systems and is configured to use Multi Factor Authentication (MFA).

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 and at rest on AWS. TLS v1.2 and higher is implemented with key exchange algorithm that supports perfect forward secrecy and provides encryption of 256 bits or stronger. Encryption at Rest is enabled across the board for all data and databases, including logs using Transparent Disk Encryption (TDE) on AWS Aurora RDS volumes.

CPA Global has policies, procedures, and mechanisms established for effective key management to support encryption of data in storage and in transmission. AWS instance leverages AWS Key Management Service (KMS) which uses Hardware Security Module (HSM) to generate, store & manage all cryptographic keys for data encryption, designed to securely store and process cryptographic key material for a wide variety of uses such as database encryption, Public Key Infrastructure (PKI), authentication and authorization.

Capacity Management

Proactive monitoring across the full stack in AWS 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.

Resilience and Recovery

**FORECAST®** exploits AWS provided infrastructure services and product capabilities to implement Active-Active fully load balanced solution and combination of health checks with Autoscaling (ASG) on Elastic Beanstalk allows self-healing capabilities within the product. Self-healing mechanisms can often be described when the ASG automatically recognize that only three servers are online when there should be four, so it stops routing traffic to the defunct server. It creates a replacement which comes back online, stabilizes it, tests to make sure the code is deployed properly, and then begins resuming routing to that server.

AWS services are designed for high availability and reliability by using Availability Zones (AZ) which if configured for multi-AZ copies the data at least across three (3) different datacenters in the same region. Availability Zones are distinct locations that are engineered to be insulated from failures in other Availability Zones. They also provide inexpensive, low-latency network connectivity to other Availability Zones in the same region. All compute and database instances in AWS for **FORECAST®** is configured for point in time recovery snapshots and replication within availability zones in the region.

**RTO and RPO**

- Recovery Time Objective (RTO) of 4 Hours.
- Recovery Point Objective (RPO) of 30 mins for data loss.
- Backup Retention period of 35 days.

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.

To read further on AWS regions and availability zones, please read https://docs.aws.amazon.com/general/latest/gr/rande.html
THANK YOU