# Abacus Private Cloud Security

Securely access all your sensitive data and vital applications from anywhere, anytime.

**APC puts your critical practice data and vital applications into a Compliance-Ready private virtual workspace, while removing IT management burdens and costs and maximizing your organization's performance.**

**Optional intro**

AbacusNext was founded in 1983 and provides mission critical, compliance-ready, fully integrated and cloud-enabled technology solutions to the legal, accounting, banking and insurance sectors.

The center piece of AbacusNext's products and services portfolio is Abacus Private Cloud (APC)-a fully integrated private cloud ecosystem that combines desktop-as-a-service, fully managed IT, and full spectrum cybersecurity with strict regulatory compliance and 24x7 technical support. APC is the center of their clients' technology universe, creating a secure digital workspace that's software agnostic and that seamlessly integrates the firm's mission critical applications and data so they're accessible anywhere, anytime, from any device.

## SECURITY

AbacusNext's APC is designed to provide a secure private environment for customers to store and access a wide variety of customer data. Built into APC as the default services is a robust suite of security services and compliance policies, such as two-factor authentication, single sign-on, five tiers of physical, network and data security, information handling and data privacy protocols all in accordance with NIST standards. By default, your data copied to geographically redundant data centers. All the services from the data floor to user access controls is audited and managed to the SOC 2 Type 2 compliance standards to ensure your business safe and protected 24 x 7.

- IPS/IDS – Intrusion Prevention Services / Intrusion Detection Services

- Access to the environment with RDP TLS 1.2 – Encrypted connections
- Client Data Encryption at rest using 256bit AES
- PaaS Database Encryption with 256bit AES
- Sophos A.V.
  - Tamper Protection
  - DCP
  - AV Lockdown
- Sophos Intercept X (Ransomware)
- 2 Factor Authentication
  Multi-factor Authentication
- DDOS Protection
- Ongoing Penetration Testing Management
- Vulnerability Management using CVSS
- Operating System & App Patch Management
- Dedicated Logging and Monitoring

## INFRASTRUCTURE REDUNDANCY

AbacusNext is the owner and operator of its own computing and storage infrastructure used for APC giving us full control and insight to need any client requirement. AbacusNext has designed, built, and optimized APC for the specific needs of our industry professionals and the software utilized in these industries. This includes all AbacusNext Software and 3rd party software. All audited and managed to the SOC 2 Type 2 compliance standards.

AbacusNext operates out of a variety of geographically dispersed data centers across three countries. Locations are setup in a Primary/Secondary configuration to ensure Disaster Recovery objectives are met. The physical components encompassing the APC ecosystem include multiple data center facilities, enterprise computing and storage infrastructure, Cisco networking equipment, and Unified Threat Management (UTM) firewalls.

# Abacus Private Cloud Security

AbacusNext has designed and built computing farms that consist of many servers clustered together for high-availability and no single point of failure. Virtual computing technologies are utilized for the virtual servers and virtual storage area networks (SAN). This provides the flexibility to move customers environments if there is a problem with the physical hardware or when it's time to upgrade.

- Compute clusters N+1
- Storage clusters 2N
- All communication fabrics are 2N (including EDGE firewalls)
- *Owner/Operator of APC
- Dedicated WAN IP
- Dedicated Firewalls

## COMPLIANCE

AbacusNext is one of the only companies to provide **enforced compliance** all the way to the user level. AbacusNext and all the Abacus Private Cloud services and support is SOC 2 Type 2 compliant and audited by CoalFire Controls. AbacusNext will maintain at all times enterprise-class security and standards protecting its Abacus Private Cloud ecosystem located in the United States, Canada, and the United Kingdom. While most cloud and software provide have a shared security and compliance standard, that means you, and your staff are ultimately responsible for the secure design, upkeep, and enforcement 24 x 7. Not only is APC providing a secure and compliant service. APC is fully compliance, managed 24 x 7, and **enforcing compliance** by including and providing system administration management at the systems level and all the way to the users level. This level of compliance is not common in the industry but given most of customer are in the highest regulated industries we made the investment to take compliance to the highest level.

AbacusNext Certifications

- SOC2 Type 2
- ISO 27001 in process

### Data Center Certifications

- SOC1 Type 2
- SOC2 Type 2
- SOC3
- MPAA
- PCI DSS - AOC
- PCI DSS – ROC
- ISO IEC 27001
- HIPAA Type 1
- Schellman confirmation of Engagement HIPAA Attestation

# MANAGEMENT

### TECHNICAL SUPPORT STAFF and EXPERTISE

AbacusNext APC operations are the combined and coordinated effort of the System & Networking Engineering, Pre-Sales, Implementation, and Support teams. These teams consist of:

### DATA PROTECTION

AbacusNext's APC is designed to provide a secure location for customers to store and access a wide variety of customer data from any desired location securely. Customers determine the nature and extent of the data that will be stored in APC. Likewise, customer's decide what users should have access to APC, as well as access to certain classifications of data once stored in APC. Additionally, APC included fully managed backups consisting of the following:

1. A dedicated team manages data backups 24 x 7. The APC support teams consist of individual teams focused on specific disciplines. The APC backup team manage and monitor the backup environment providing around the clock protection and access to your data.

2. All data is encrypted with 256-bit encryption that uses a 256-bit key to encrypt and decrypt backup data or files. It is the most secure encryption standard.
3. 3-2-1 Backup Rule: By default, APC includes 3-2-1 backups that include;
    a. Three (3) copies of your data:
        1) Production data
        2) Backup at the primary data center
        3) Backup replication to geographic diverse data center.
    b. Two (2) backup copies on different storage media
    c. One (1) of them located offsite (secondary data center)

## APC System & Networking Engineering

This department encompasses Network, Virtualization, Automation, Identity, Data Protection and other specialized Systems Engineers that support the underlying APC platform. This department acts as an escalation point for all other APC operational departments and provides 24/7/365 mission critical coverage to ensure the maintenance of service level commitments.

## APC Pre-Sales Engineering

Pre-Sales Engineers work with prospective clients to understand the technical needs of their business and design APC solutions that are tailored to meet them. Engineers will do a full technical assessment of your current environment at no cost to you. The technical assessment will provide a full report of computing environment and health which includes the following:

1. A full security assessment with your security vulnerability scope and corrective actions
2. Full inventory of your current computing, storage space,
3. Full inventory of your operating systems and all application.

Engineers on this team coordinate closely with the clients account rep and subsequent implementation project manager and team, to ensure clients APC solution and subsequent deployment are aligned at all phases.

# Abacus Private Cloud Security

## APC Implementation Engineering

The implementation engineering team is directly responsible for the onboarding of new clients to the APC environment. This includes configuration of user access and roles, data migration (subject to an additional fee for complex migrations), application deployment, device integration and post migration support.

- Dedicated Logging
- Dedicated Monitoring
- Dedicated Identity Management Solutions
- Company-wide 2 Factor Authentication when accessing client environments Multi-factor Authentication
- Single Sign On (SSO)
- Global Support
- Technical Account Manager (TAM)