

Palaamon

Quality & Compliance

Two Pager

-2019-



Palaamon

Quality & Compliance

Two-Pager

Physical and Logical Security Features

Llaama, November 2019

Version 2019.12.002

Llaama SAS
KM0 - Espace AKC
Rue Spoerry, 30
68100 Mulhouse
France
info@llaama.com
www.llaama.com

Palaamon Quality & Compliance

The Palaamon platform is envisioned to serve the biopharmaceutical and healthcare industries and therefore has been engineered from inception to comply with regulations such as Good Clinical Practice (GCP), HIPAA, and GDPR.

Our distributed ledger technologies are inherently suited for such compliance in that they enhance the transparency, auditability, and security of transactions made on the platform.

Distributed computing and containerization combined with unique signatures of all processes is the keystone not only to our value proposition of data immutability and reproducibility, but also of our security and privacy capabilities.

Speed of transmission lessens windows of vulnerability. Full audit trails guarantee traceability at any stage of review. Smart contracts govern data security and access, or even specify data deletion, enabling trust for collaboration. And the inherently decentralized system is prohibitive to single-point failure or dedicated attack.

Security

To ensure data availability, integrity, and confidentiality, Llaama has carefully implemented physical and logical security and privacy features in the Palaamon environment. Our engineers adopt software development and change management best practices. Risk Assessment begins at the design phase with compliance review and updates throughout operational phase.

Hosting

Palaamon is currently hosted by OVH, the gold standard for cloud computing compliance, which provides high security standards in its data centers following their certified ISMS (ISO 27001, SOC 1, SOC 2., OVH is compliant with GDPR and also holds a STAR certification from the Cloud Security Alliance (CSA).

The employed data centers feature state-of-the-art security and environmental controls as well as redundancy and backup.

Access to all data center premises is strictly monitored. Data center boundaries are secured with barbed wire fencing to prevent intrusions or hazards. Video surveillance and motion detection systems are in continuous operation. Physical activity in the data centers and outside the buildings is also monitored and recorded on secure servers. A surveillance team is on site 24/7/365.

Strict security procedures have been put in place to control and monitor access to the premises. The data centers have an even higher level of protection, and only a very limited number of authorized personnel can gain entry.

Network Architecture

Data is end-to-end encrypted, protected by advanced firewalls, and every application is published by a reverse proxy with a web application firewall.

Our provider builds its network in a redundant manner; multiple security measures minimize any risk of failure. The redundancy of links also enables data to take the shortest path and benefit from minimum latency.

All services include protection against every type of DDoS attack. Three 160 Gbps Anti-DDoS infrastructures have been set up in the key global data centers. Our provider is capable of mitigating up to 4Tbps, 24/7/365.

Account Security

To help ensure that only authorized users and processes access your Palaamon account, Llaama provides credentials for access control, HTTPS endpoints for encrypted data transmission, user-activity logging for security monitoring, and security checks.

Authentication credentials include complex passwords, cryptographic keys, digital signatures, and certificates. We also provide the option of requiring multi-factor authentication (MFA) to log into your Palaamon Account.

Conclusion

Llaama is proactive with regard to sustainable quality and compliance.

However, it remains incumbent upon Palaamon customers to consult with their own advisors to ensure that company internal policies and procedures are suitable for current IT, software, GxP, and security practices using Palaamon. Llaama's part in this shared responsibility includes providing its services on a highly secure and controlled platform and providing a wide array of security features.

For more detailed compliance and security information, please always consult our full Compliance White Paper, the latest version of which can be found at www.llaama.com.