em Editorial Manager®

pm ProduXion Manager®

Infrastructure Overview for Editorial Manager® and ProduXion Manager®

Editorial Manager® and **ProduXion Manager®** utilize a robust AWS cloud infrastructure, strategically designed to enable seamless workload transfers or redeployments in the event of performance issues or outages, ensuring continuous and reliable service.

Key Features of Our Infrastructure:

✓ **Auto-Scaling Asynchronous Server Architecture:** Our system is designed to handle processor-intensive tasks without compromising response times.

✓ **Scalability:** By utilizing AWS infrastructure, we achieve near-infinite scalability to meet the varying demands of scholarly journal operations.

✓ **Continuous Monitoring:** Continuous monitoring of all cloud resources to optimize performance and respond proactively to any potential issues.

✓ **Global Performance Monitoring:** A global network of agents monitor performance worldwide, supported by 24/7/365 coverage from Aries' technical teams.

✓ **User Access Controls:** Adhering to the principle of least privilege ensures employees have access only to the resources essential for their specific job functions, reducing potential security risks while preserving operational efficiency.

✓ **Incident Management Process:** Our incident management process provides 24/7/365 support to ensure swift responses and minimize downtime. Comprehensive procedures are in place to identify, escalate, and resolve incidents efficiently.

✓ **Annual Technical Resilience & Data Recovery Testing** includes:

Data Integrity Recovery Plan (DIRP): A comprehensive recovery process for data corruption or deletion, primarily utilizing backup and restoration methods.
System Recovery Plan (SRP): Protocols for recovering from component failures that necessitate failover to an alternate environment.
Product Recovery Plan (PRP): Procedures for recovering from cyber-attacks or outages, which involve rebuilding or re-platforming source code and data in a new, secure environment.

✓ **Regular Security and Compliance Training:** All staff is required to undergo regular security and compliance training, ensuring they are informed about best practices, regulatory requirements, and the latest security threats. This empowers staff to contribute to the overall security posture of the organization.

✓ **Customer Communication Procedures:** Established protocols protocols to notify customers and users promptly about any scheduled or unexpected downtime.

✓ **Third-Party Audits:** Regular third-party security, infrastructure, and application audits, along with monthly penetration testing to identify and mitigate vulnerabilities.

✓ **Code Validation:** Modern code scanning tools ensure that all application and infrastructure code is validated for security before deployment.

✓ **Automated Patching:** Monthly automated infrastructure patching to maintain security and stability.

Powered by: Aries systems.