



Hosting Checklist

| ✓ | Servers mirrored across geographically separate data centers to ensure continuity of service in the event of disaster such as local fire or explosion. |
|--------------|---|
| ✓ | Dual, high-bandwidth (T3) connections from different Internet vendors to ensure continuity of service in the event of vendor service outage. |
| ✓ | Scalable and tiered Asynchronous Server Architecture to ensure that system response is not negatively impacted by processor-intensive tasks (e.g. building PDFs). |
| ✓ | Local, dedicated, power generators at each data center to ensure continuity of service in the event of power outage. |
| \checkmark | Infrastructure capacity to address the needs of 8,500+ scholarly journals. |
| ✓ | Continuous monitoring of network activity and performance to ensure optimal security and responsiveness. |
| ✓ | System Monitoring and Reporting Tool (S.M.A.R.T) continuously monitors "probe points" to ensure system health. |
| ✓ | 24x7x365 IT and Engineer staff coverage. |
| ✓ | Written procedures and protocols for mission critical data center activities with management reporting and escalation of any system anomalies. |
| ✓ | All uploaded submission files virus checked by Norton AntiVirus and Norton's Enterprise Management tools. |
| \checkmark | Hardened data centers with dual factor, biometric access control. |
| ✓ | RSA SecurID two factor token authentication for access to LAN from external WAN environments. |
| ✓ | Documented procedures for contacting customers and users in the event of any system scheduled or unscheduled down time. |
| \checkmark | Track record of high system availability (99.99%). |
| ✓ | Risk mitigation strategy for deployment of new software, by incrementally releasing new software to groups of journals rather than high-risk 'big bang' approach. |
| \checkmark | Periodic third party security and infrastructure audits. |
| ✓ | Customer data center auditing rights. |

