

INGENUITY SECURITY

Overview

The need to protect internal and proprietary information and data against unauthorized access is a key concern for many life science research institutions. Ingenuity Systems deploys world-class technologies and processes to ensure the security of customer data. These measures are regularly reviewed, maintained, and updated to ensure that research performed with Ingenuity products and services remains uncompromised.

Security Measures

Security measures deployed today include the following:

- **Session Encryption:** The IPA application is accessed from the Internet through 256-bit AES encrypted sessions.
- **Network Security:** The network is designed to use multiple firewall layers for security. Network data flows are further safeguarded by network and port address translation, and non-routable IP addressing schemes. System-level access is designed to only be gained through private management circuits by Ingenuity administrators, whose management systems reside on networks at Ingenuity headquarters. Network firewall and other security device logs are monitored by Ingenuity administrators to identify security threats.
- **Systems Security:** IPA servers are single-purposed and hardened to minimize the number of access points. Operating system, service and application patch levels are maintained per vendor recommendations and Ingenuity risk assessment. Administrative account password complexity and password change frequency mechanisms ensure only authorized personnel are able to gain system level access to servers.
- **Application User Authentication:** IPA users are authenticated through username and passwords. Initial passwords are randomly generated and must be changed after initial login, and password complexity rules are enforced. Accounts will automatically lock out after multiple unsuccessful login attempts to avoid hacker "dictionary attacks".
- **Application Data Security:** The IPA database model is designed to prevent one IPA user from unauthorized access to another IPA user's workspace.
- **Physical Security:** IPA systems are located in a facility monitored at all times by guards and video surveillance. Access is restricted to authorized personnel possessing picture identification. Within the facility, IPA systems are located in a secured cage.
- **Backups/Disaster Recovery:** Backups of production customer data are performed regularly to backup disks and magnetic tape. Backup tapes are moved to secure storage on a regular basis. At the customer's option, data is replicated to a disaster recovery facility to minimize the impact of data loss from a catastrophic event and to enable us to recover quickly.
- **Personnel:** The IPA operations team includes staff with security training and certifications including SANS GCIA, Cisco CCSP, and the ISO recognized CISSP security certification.

Contact

If you have any questions or concerns about security, please contact your Ingenuity Account Executive. If you don't have contact information for your representative, you can email sales@ingenuity.com.