CYBER SECURITY

Alaris works diligently to ensure the safety of our clients and their work. The facts listed below are some of the security measures we have established to safeguard all your information and material.

Network Security

- Up-to-date firewalls are equipped with malware and content filtering to reduce risk of exposure.
- Network file access is on a need-to-know basis, and files are actively backed up in real time.
- Servers offer 99.999% uptime and are stored offsite in secure 24-hour manned facilities with restricted access.
- Alaris offers managed guest Wi-Fi capability, while maintaining our data network security.
- Network tools filter internet content including social media, streaming services and personal sites.
- After 5 login attempts, users are locked out until reset by a network administrator.
- Email is monitored for spam, phishing attacks and malware, and has strict file attachment rules.
- Network files are backed up offsite and are restorable up to two weeks in the event of an attack.

Software Security

- Anti-virus software is installed, maintained and updated daily on all machines.
- Zoom cloud-based videoconference software enables clients to connect securely and share content in restricted virtual meeting rooms.
- Alaris utilizes secure methods of file transfer; ShareFile, Dropbox, and private SFTP.

Security Policies

- No Personally Identifiable Information is stored as a hard copy.
- All electronic records are deleted after seven years.
- Alaris certifies the destruction of all hardware containing PII.
- All subcontractors sign BAAs, confidentiality and communications agreements with Alaris.
- Our employees undergo training on security and confidentiality of all data.
- We hold extensive data breach insurance coverage in excess of the industry standard.