October 25, 2023

To Whom it may Concern:

Aras has established the following Information Security Policies for the purposes of protecting the confidentiality, integrity, and availability of Aras information systems and data:

- Acceptable Use and Protections (AUP) Policy
- Access Control Policy
- Asset Management Policy
- Audit and Accountability Policy
- Change Management Policy
- Configuration Management Policy
- Data Classification and Asset Protection Policy
- Human Resources and Training Policy
- Incident Response Policy
- Information Security Policy
- Information Security Management System (ISMS) Policy
- Physical Security and Data Center Maintenance Policy
- Recovery Policy
- Risk and Compliance Management Policy
- SDLC Policy
- System and Communications Protection Policy
- System and Information Integrity Policy
- Vendor Management Policy

It should be noted that the Aras Information Security and Compliance Program and its associated Policies and Procedures are classified as Internal Confidential and therefore are not to be shared with outside entities. Aras Information Security Policies were built in alignment with industry best practices, standards, and frameworks such as ISO 27001 and CMMC 2.0/NIST 800-171. Policies are reviewed annually at a minimum and validated by independent, third-party auditors in conjunction with our security certification audits.

Signed,

Aras Information Security and Compliance Team