TECOLOTE
RESEARCH

SOFTWARE PRODUCTS/
SERVICES GROUP

5383 Hollister Avenue, Suite 100 | Santa Barbara, CA 93111-2304 | phone 805.964.6963

MEMORANDUM FOR: ACEIT Users

FROM: Tecolote Research Inc.

SUBJECT: ACEIT Software Development Security Support Statement
Date: 7 April 2023

Tecolote Research Inc. (Tecolote) recognizes the importance of an effective security program to protect the company's employees, assets, information, integrity, and reputation from potential threats. In support of Tecolote's various development environments Tecolote employs a variety of software development methods, best practices, and checks and balances to ensure the integrity of the software and development services we sell.

The company commitment is guided by the basic core values, code of conduct, and business ethics which shape and influence the way Tecolote operates. These core values include professionalism, respect for employees and stakeholders, and a permanent concern for products and services we sell.

This software development security support statement is aimed at providing you with more information about our security infrastructure and practices.

- We follow a defined methodology for developing secure software that is designed to increase the resiliency and trustworthiness of our products. Our products are deployed on an iterative, rapid release development lifecycle. Security and security testing are implemented throughout the entire software development methodology. Quality Assurance is involved at each phase of the lifecycle and security best practices are a mandated aspect of all development activities.

- Tecolote maintains a software change management process to ensure that all changes made to the production environment are applied in a deliberate manner. Changes to information systems, and other system components, and physical and environment changes are monitored and controlled through a formal change control process. Changes are reviewed, approved, tested, and monitored post-implementation to ensure that the expected changes are operating as intended.

- Tecolote developers review all code with consideration for security vulnerabilities and other best practices.

- Tecolote regularly audits and monitors various sources for Common Vulnerabilities and Exposures (CVE) reports associated with all development components. Every effort is taken mitigate the risk to the development environment.

- Tecolote complies with NIST 800-171, CMMC, C-SRCM as required by DFAR, GSA, and DMCA.

This policy is subject to annual review and is amended as necessary to ensure that it continues to be appropriate to the needs of the business. The Tecolote software development management team is responsible for ensuring that this information security policy is communicated and understood by all developers.

Respectfully,

Melissa Cyrulik
ACEIT Program Manager