Issue date: 14 November 2023
Valid until: 2 November 2028

NO: SAMM 856

LABORATORY LOCATION:
(PERMANENT LABORATORY)

TÜV AUSTRIA CYBERSECURITY LAB SDN. BHD.
A-11-01, EMPIRE OFFICE TOWER
SS16/1, SUBANG JAYA
47500 SUBANG JAYA
SELANGOR DARUL EHSAN
MALAYSIA.

FIELD(S) OF TESTING:

SOFTWARE TESTING
INFORMATION TECHNOLOGY SECURITY EVALUATION AND TESTING: COMMON CRITERIA

This laboratory has demonstrated its technical competence to operate in accordance with MS ISO/IEC 17025:2017 (ISO/IEC 17025:2017).

This laboratory's fulfillment of the requirements of ISO/IEC 17025 means the laboratory meets both the technical competence requirements and management system requirements that are necessary for it to consistently deliver technically valid test results and calibrations. The management system requirements in ISO/IEC 17025 are written in language relevant to laboratory operations and operate generally in accordance with the principles of ISO 9001 (see Joint ISO-ILAC-IAF Communiqué dated April 2017).

SCOPE OF TESTING: SOFTWARE TESTING

Materials/ Product Tested	Type of Tests/ Properties measured/ Range of Measurement	Standard Test Methods/Equipment/Techniques
Web Application	Web Application Penetration Testing (WAPT) to identify vulnerabilities such as: - Broken Access Control - Cryptographic Failures - Injection - Insecure Design - Security Misconfiguration - Vulnerable and Outdated Components - Identification and Data Integrity Failures - Software and Data Integrity Failures - Security Logging and Monitoring Failures - Server-side Request Forgery (SSRF)	Web application penetration test method: - Open Web Application Security Project (OWASP)
Mobile Application	Mobile Application Penetration Testing (MAPT) to identify vulnerabilities such as: Open Web Application Security Project - Improper Platform Usage - Insecure Data Storage - Insecure Communication - Insecure Authentication - Insufficient Cryptography - Insecure Authorization - Client Code Quality - Code Tampering - Reverse Engineering - Extraneous Functionality	Mobile application penetration testing methods: - Open Web Application Security Project (OWASP) - Open Android Security Assessment Methodology (OASAM)

SCOPE OF TESTING: SOFTWARE TESTING

Materials/ Product Tested	Type of Tests/ Properties measured/ Range of Measurement	Standard Test Methods/Equipment/Techniques
Mobile Application	Mobile Application Penetration Testing (MAPT) to identify vulnerabilities such as: Open Android Security Assessment Methodology - Information Gathering - Confirmation and Deploy Management - Authentication - Cryptography - Information Leak - Data Validation - Intent Spoofing - Unauthorized Intent Reception - Business Logic	Mobile application penetration testing methods: - Open Web Application Security Project (OWASP) - Open Android Security Assessment Methodology (OASAM)
Network servers, network devices, network security devices and IoT	Vulnerability Assessment and Penetration Testing (VAPT) to identify vulnerabilities such as: - SSL/TLS Certificate, Cipher Algorithms and Protocols - Obsolete Version, EOL (End of Life) findings - Patch-related findings for Operating Systems, Applications and Services - Best practices and Configuration findings for Known Services - Authentication based findings	Vulnerability assessment and penetration testing method: - Open Source Security Testing Methodology Manual (OSSTMM)
Application Source Code	Source Code Review (SCR) to audit the source code for an application flaw such as: - Injection Flaws - Broken Authentication and Session Management - Cross-Site Scripting (XSS) - Insecure Direct Object Reference - Security Misconfiguration - Sensitive Data Exposure - Missing Functional Level Access Control - Cross-Site Request Forgery (CSRF) - Using Components with Known Vulnerabilities - Unvalidated Redirects and Forwards	Source code review method: - Open Web Application Security Project (OWASP)

Signatory:

1. **Fow Chee Kang**

Issue date: 14 November 2023
Valid until: 2 November 2028

NO: SAMM 856

SCOPE OF TESTING: INFORMATION TECHNOLOGY SECURITY EVALUTION AND TESTING: COMMON CRITERIA

Materials/ Product Tested	Type of Tests/ Properties measured/ Range of Measurement	Standard Test Methods/Equipment/Techniques
Protection Profile and ICT products and systems which include Firmware and Software such as low level drivers, operating systems and applications	Information Security Evaluation of IT security under the MyCC Scheme in accordance with information Technology Security Evaluation Criteria ISO/IEC 15408, "Information technology – Security techniques – Evaluation criteria for IT"	Common Criteria for Information Technology Security Evaluation (CC v3.1) including: • Part 1: Introduction and general model • Part 2: Security functional requirements • Part 3: Security assurance requirements Common Methodology for Information Technology Security Evaluation (CEM v3.1) The Common Criteria Evaluation for the following Assurance Level: • EAL1: Functionally Tested • EAL2: Structurally Tested • EAL3: Methodically Tested and Checked • EAL4: Methodically Designed

Signatory:

1. **Fow Chee Kang**