TQCS INTERNATIONAL PTY LTD
ACN 100 435 916

PO Box 483, Woodville, SA 5011 Australia
p: 61 8 8347 0603 f: 61 8 8445 9423
e: info@tqcsi.com www.tqcsi.com

POLICY FOR AUDITING & CERTIFICATION TO ISO/IEC 27001

In addition to the General Policy which applies to all Standards, this policy describes interpretations of the requirements for auditing and certification of information security management systems to ISO/IEC 27001 made by TQCSI's Certification Approval Panel. It complements TQCSI Work Instruction 44 (ISO 27001) which should also be referred to by auditors when auditing clients' information security management systems.

A **minor nonconformance** is to be raised where:

- a discrepancy which has the potential to have a significant impact on the effectiveness of the ISMS has not been addressed since being raised at a previous audit
- a serious discrepancy or a number of like discrepancies indicate there is a breakdown in part of the information security management system or the security of information is jeopardised
- the objectives of the information security management system are not established or monitored
- there is a significant breach of legislation or a regulatory requirement
- there is an ISMS hazard that is not controlled and could cause a breach of security.

A **major nonconformance** is to be raised where:

- the agreed action plan to address a minor nonconformance has not been implemented
- a serious discrepancy or a number of like discrepancies indicate there is a total breakdown in the ISMS or there is direct evidence of high risk of serious injury or death, substantial financial losses or cessation of business activities
- there is a very serious ISMS risk /threat that is not controlled and could cause a serious breach of security and poses threat to assets, vulnerabilities and impacts
- there is a very significant breach of legislation or a regulatory requirement.

General:

- ISMS related objectives must be identified, documented and reviewed in a plan.
- ISMS controls are selected and implemented, and are consistent with ISO/IEC 27001, Annex A.
- Management approval of risk must be obtained.
- Clients are expected to review the reference controls implemented as described in the Statement of Applicability at a frequency based on the risk of each reference control objective. If no frequency is documented, 12 monthly intervals are expected.

Approved: ***original signed***

Craig Bates
Managing Director & President, TQCSI

Date: 26 September 2024