EQA Information Security Regulations

This document is Supplemental to the EQA Scheme Regulations. It is designed to cover the extra requirements for ISO/IEC 27001:2017 Certification.

Information Security Legislation:

1. Within their Information Security Policy, organisations are expected to include a commitment to satisfy all applicable requirements, including compliance with all relevant legislative statutory and regulatory requirements. Failure to meet this commitment or failure to take action to meet this commitment within a reasonable time frame will result in suspension and/or withdrawal of certification by EQA.
2. Organisations are obliged to inform EQA of any breaches of Information Security Legislation without delay. EQA will conduct a review of the certification status based on the severity of the occurrence and any remedial actions which have been taken to rectify the situation.
3. Organisations are obliged to inform EQA of any litigious action being taken against them for breach of Information Legislation without delay.

Internal Audit and Management Review

1. EQA will not certify an organisation's information security management system (ISMS) unless there is evidence that the organisation has operated through at least one management review and one internal ISMS audit covering the organisation's scope of certification.

Access to Organisational Records

1. Organisations shall make all necessary arrangements for the access to internal audit reports and reports of independent reviews of information security. During Stage 1 of the certification audit, organisations shall make the following available to the audit team:
    a. General information concerning the ISMS and the activities it covers
    b. A copy of the required ISMS documentation specified in ISO/IEC 27001, as well as associated documentation.
2. Before any certification audit, organisations will be asked to report if any ISMS-related documented information cannot be made available for review by the audit team owing to confidential or sensitive information contained within. In the absence of such information, EQA will determine whether the ISMS can be adequately audited. If EQA concludes that it is not possible to adequately audit the ISMS without reviewing the identified confidential or sensitive information, the organisation in question will be advised that the certification audit cannot take place until appropriate access arrangements are granted.
3. Where a certification audit cannot take place, EQA may elect to invoke Clause 15 of the EQA Scheme Regulations concerning 'Withdrawal, Refusal and Suspension of Certification'.