**QG Information Security Management Standard**

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Section | Standard | Deliverables |
| 1 | Information Security Management Policy | A documented Information Security/Information Assurance Policy is in place | An IS/IA policy is written and includes;   * + Management commitment,   + Scope of system,   + Meeting external standards,   + Communication channels,   + Dated   + Signed   The policy has been reviewed in the last 12 months |
| 2 | Scope | A statement is in place that defines the scope of the system. | The statement includes   * + Locations   + Other standards in scope |
| 3 | Management Responsibilities | Management responsibilities are defined in writing | Organisation ownership is defined, in writing and by section  Evidence is in place that individuals understand that they have section responsibility  A management representative is identified |
| 4 | Security Objectives | Company security objectives are documented, agreed and reviewed | A written system is in place that details;   * + objectives,   + scope   + definitions   A system is in place that reviews and updates objectives on a regular basis (minimum yearly) |
| 5 | Legal Requirements | A process is in place that documents and reviews legal requirements | A process is in place to document   * + legal requirements,   + Security regime,   + Security rules   + Security responsibilities   + Data Protection |
| 6 | Communication | A system is in place to communicate information security policies | A system is in place to communicate with   * + Internal stakeholders   + External stakeholders |
| 7 | Operational Control | A system is in place to manage and control operational processes | A system is in place that covers   * Security Risk Assessments * Physical * Online * Incident Management, Disaster Recovery & Business Continuity * Detection * Resolution * Recovery * Asset Controls |
| 8 | Procurement | A system shall be in place to identify and monitor suppliers | A documented system is in place to monitor supplies of goods and services.    The system identifies the risks associated with each procurement process. |
| 9 | Incident Preparedness | A system is in place to manage and control unplanned incidents | A documented system is in place that covers   * Risk identification * Key contacts * Review & revision |
| 10 | Checking & Document Control | A system is in place for checking and document control | A documented system is in place to cover the following   * Measuring * Monitoring * Evaluation * Non-conformity * Corrective action * Preventative action * Control of records   + Identification   + Storage   + Protection   + Retrieval   + Retention   + Disposal |
| 11 | People & Training | A system is in place to manage and measure training processes | A system is in place to identify training needs of employees and is implemented on. The system covers;   * Pre-employment * Recruitment * Induction   A HR System is in place that covers;   * + Security awareness   + Security risks   + Whistleblowing   + Disciplinary * Records |
| 12 | Management Review | A system is in place to review the effectiveness of the ISMS | A system that reviews   * Policy * Objectives   On an annual basis is documented and acted upon |
| 13 | Audit | An internal and/or third part audit is carried out at regular intervals. | An audit process is in place that checks the system at least once per year. |