Requirements for a QG-Information Security Management System - Questionnaire

**Introduction**

The QG Information Security Management Standard is recommended for organisations looking for a foundation level of Information Security Management System where the risk of a change would only minimally affect the customers/supplier/partner relationship. It is mainly applicable where business systems are straightforward and consistent (wholesaler, retailer) or that another governing body oversees the system, for example accountants, solicitors, engineers.

The main objective of the Information Security Management assessment is to determine that your organisation has effectively implemented the systems required by the Scheme, in order to minimise inconsistency of your supply or service.

The completed questionnaire attests that you meet the Requirements of the Information Security Management Standard, which must be approved by a Board member or equivalent, and will then be verified by a competent assessor from **QG Business Solutions** (the Certifying Body). Such verification may take a number of forms, and could include, for example, a telephone conference. The verification process will be at the discretion of **QG Business Solutions.**

**Scope of Information Security Management Standard**

The Scope is defined as the areas that will have an affect on your customer relationship. This scope will be printed on your certificate of compliance.

You will be required to identify the actual scope of the system to be evaluated as part of the questionnaire.

**How to avoid delays & additional charges**

You may incur additional charges if details are not sufficiently supplied, answer the questions as fully as possible giving supporting comments, paragraphs from policies and screen shots where possible. As a rule of thumb if it takes longer to assess the submission than you spent preparing it, you may be charged.

**Organisation Identification**

Please provide details as follows:

|  |  |
| --- | --- |
| Organisation Name (legal entity): |  |
| Sector: |  |
| Parent Organisation name (if any): |  |
| Size of organisation micro, small, medium, large.  (See definition below) |  |
| No of employees |  |
| Point of Contact name:  Salutation (Mr, Mrs, Miss etc)  Initial  First  Surname |  |
| Job Title: |  |
| Email address: |  |
| Telephone Number: |  |
| Main web address for company in scope: |  |
| Building Name/Number  Address 1  Address 2  Address 3  City  County  Postcode |  |
| Certification Body: |  |
| Do you wish to be **excluded** from the register of QG Management Systems certified companies. Exclusion means customers will not be able to find your entry. If this is left blank you will be entered. |  |
| From time to time QG Business Solutions and other interested bodies may wish to use your company for marketing the QG Management Standards. If you wish to be promoted in this way please enter **YES** in the box. |  |

**SME Definition**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Company category** | **Employees** | **Turnover** | or | | **Balance sheet total** |
| Medium-sized | < 250 | ≤ € 50 m | | ≤ € 43 m | |
| Small | < 50 | ≤ € 10 m | | ≤ € 10 m | |
| Micro | < 10 | ≤ € 2 m | | ≤ € 2 m | |

**Business Scope**

For the purposes of the Information Security Management Standard the scope should include all those parts of the business that affects your customer/suppliers and partners.

Please identify the scope of the system to be assessed under this questionnaire, including locations.

|  |
| --- |
|  |

1. Information Security/Assurance Management Policy

Objective

To publicly declare the information security values and of the company.

|  |  |  |
| --- | --- | --- |
|  | Requirement | Evidence/Narrative |
| 1 | Does the organisation have a written Information Security/Assurance Policy? |  |
| 1.1 | Does it define the management’s commitment? |  |
| 1.2 | Does it define the scope of the system |  |
| 1.3 | Does it define which external standards it meets? |  |
| 1.4 | Does it define how it is communicated to staff, customer, suppliers and partners? |  |
| 1.5 | Has it been reviewed in the last 12 months, signed and dated by a senior member of staff? |  |
| Action | Please attach IS/IA policy |  |

1. Scope

Objective

To define to interested parties the length and breadth of the assessed system

|  |  |  |
| --- | --- | --- |
|  | Requirement | Evidence/Narrative |
| 2 | Is there a statement that identifies the areas of the organisation that the assessment relates to? |  |
| 2.1 | Does it define locations |  |
| 2.2 | Does it define other standards in scope? |  |

1. Management Responsibilities

Objective

To ensure the organisations management know their responsibilities for Information Security Management.

|  |  |  |
| --- | --- | --- |
|  | Requirement | Evidence/Narrative |
| 3 | Are management responsibilities defined in writing? |  |
| 3.1 | How do managers understand what their responsibilities are? |  |
| 3.2 | Who is the Management Representative? |  |

1. Security Objectives

Objective

To measure the effectiveness and improvement of the organisations security regime.

|  |  |  |
| --- | --- | --- |
|  | Requirement | Evidence/Narrative |
| 4 | Is there documented security objectives in place? |  |
| 4.1 | Does it define the scope? |  |
| 4.2 | Do they include definitions? |  |
| 4.3 | Is it reviewed regularly |  |

1. Legal Requirements

Objective

To ensure that the organisation is adhering to up to date legal requirements.

|  |  |  |
| --- | --- | --- |
|  | Requirement | Evidence/Narrative |
| 5 | Has the organisation identified, documented and implemented all security legislation pertaining its sector? |  |
| 5.1 | Does the document include the security regime? |  |
| 5.2 | Does the document include security rules? |  |
| 5.3 | Does the document include security responsibilities? |  |
| 5.4 | Does it the document include Data Protection legislation? |  |

1. Communication

Objective

To ensure the whole organisation, it’s suppliers and partners understands the importance of Information Security.

|  |  |  |
| --- | --- | --- |
|  | Requirement | Evidence/Narrative |
| 6 | Does the organisation have a system in place to communicate Information security issues? |  |
| 6.1 | Does the organisation have a system in place to communicate Information Security issues internally? |  |
| 6.1 | Does it have a system in place to communicate Information Security issues externally? |  |

1. Operational Control

Objective

To ensure that the organisations operational processes associated with information security are understood and kept under control.

|  |  |  |
| --- | --- | --- |
|  | Requirement | Evidence/Narrative |
| 7 | Does the organisation have a system in place to manage and control operational processes? |  |
| 7.1 | Does it include security risk assessments? |  |
| 7.2 | Does it cover physical security processes? |  |
| 7.3 | Does it have an incident management, disaster recovery & business continuity plan in place (may be one document)? |  |
| 7.4 | Does it define the process for detection of breaches? |  |
| 7.5 | Does it define resolution processes? |  |
| 7.6 | Does it state how recovery will take place? |  |
| 7.7 | Does it understand it’s assets and do you have asset controls in place? |  |

1. Procurement

Objective

To ensure that procured goods and services are fit for purpose.

|  |  |  |
| --- | --- | --- |
|  | Requirement | Evidence/Narrative |
| 6 | Does the organisation have a system in place that identifies and monitors key suppliers? |  |
| 6.1 | Does it identify the risks associated with each supplier? |  |

1. Incident Preparedness

Objective

To ensure that should a situation arise the organisation has procedures in place to deal with it.

|  |  |  |
| --- | --- | --- |
|  | Requirement | Evidence/Narrative |
| 9 | Has the organisation identified potential incidents that may take place? |  |
| 9.1 | Has it identified the risks associated with potential incidents? |  |
| 9.2 | Has it identified key contacts should an incident take place? |  |
| 9.3 | Is the system reviewed and revised on a regular basis? |  |

1. Checking and Document Control

Objective

To ensure the organisation has a system in place to manage documentation.

|  |  |  |
| --- | --- | --- |
|  | Requirement | Evidence/Narrative |
| 10 | Does the organisation have a document management system (DMS) in place? |  |
| 10.1 | Has the organisation implemented a documented systematic approach for measuring and monitoring it’s Information Security/Assurance DMS? |  |
| 10.2 | Does it evaluate it’s compliance? |  |
| 10.3 | Has it implemented a system for non-compliance, corrective and preventative action? |  |
| 10.4 | Does the DMS Identify the documents owners? |  |
| 10.5 | Does it identify where they are stored? |  |
| 10.6 | Has the organisation implemented a document protection system? |  |
| 10.7 | Does it state retention periods? |  |
| 10.8 | Has the organisation a formal retrieval process in place? |  |
| 10.9 | Does the DMS identify how to deal with documents that are superseded? |  |

1. People & Training

Objective

To ensure that employees have the authority, capability and experience to deliver services to the required standard

|  |  |  |
| --- | --- | --- |
|  | Requirement | Evidence/Narrative |
| 11 | Are the training needs of all staff assessed to ensure that they are competent and/or qualified to carry out their duties effectively and safely within the business? |  |
| 11.1 | Is there a recruitment process in place that covers all levels of the organisation? |  |
| 11.2 | Does the process cover pre-employment checks? |  |
| 11.3 | Does the process cover induction? |  |
| 11.4 | Is there an HR process? |  |
| 11.5 | Does the HR process include security awareness training? |  |
| 11.6 | Does the HR process include guidance on security risks? |  |
| 11.7 | Does the HR process include a whistleblowing policy? |  |
| 11.8 | Does the company disciplinary procedure include internal security |  |
| 11.9 | Are training records kept and kept up to date for all staff? |  |

1. Management Review

Objective

To ensure that the management of the organisation have all the controls in place to manage information effectively.

|  |  |  |
| --- | --- | --- |
|  | Requirement | Evidence/Narrative |
| 12 | Does the organisations management review the effectiveness of the Information Security Management System at least once a year to ensure its effectiveness. |  |
| 12.1 | Is the review documented? |  |

1. Audit & Assessments

Objective

To ensure that systems are audited for compliance

|  |  |  |
| --- | --- | --- |
|  | Requirement | Evidence/Narrative |
| 11 | Are internal and/or third part audits carried out at regular intervals? |  |
| 11.1 | Is a documented audit process is in place that checks the system at least once per year. |  |

**Approval**

It is a requirement of the Scheme that a Board level (or equivalent) of the organisation has approved the information given. Please provide evidence of such approval:

When you have completed the document you should email it to;

|  |
| --- |
| Brian Lightowler |
| 01228 631681 |
| [blightowler@qgbiz.co.uk](mailto:blightowler@qgbiz.co.uk)  REMEMBER TO ENSURE IT HAS BEEN SIGNED BY A SENIOR MEMBER OF YOUR COMPANY. |