GRD
buiding contractors limited

Information Security Policy

Objective

We aim to ensure business continuity in the face of unforeseen security issues and to and minimise damage by preventing and reducing the impact of such incidents.

Notes

- Information takes many forms and includes data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes or diskettes or spoken in conversation or over the telephone.

- The protection of valuable or sensitive information from unauthorised disclosure or intelligible interruption.

- Safeguarding the accuracy and completeness of information by protecting against unauthorised modification.

- This applies to record keeping and most controls will already be in place. It includes the requirements of legislation such as the Data Protection Act, Freedom of Information Act etc

Policy

The purpose of the Policy is to ensure the confidentiality, integrity and availability of its information is maintained by implementing best practice to minimise risk.

It is the policy of the company to ensure that:

- Information will be protected against unauthorised access

- Confidentiality of information will be assured

- Integrity of information will be maintained

- Regulatory and legislative requirements will be met

- Information Security Training will be provided

- All breaches of Information Security, actual or suspected, will be reported and investigated

- Standards will be produced to support the policy

- Business requirements for the availability of information and information systems will be met

- All Managers are directly responsible for implementing the policy within their business areas, and for adherence by their site operatives
- It is the responsibility of each employee to adhere to the Information Security Policy

Need for a Security Policy

The data stored in manual and electronic systems used by GRD represent an extremely valuable asset. The increasing reliance on information technology for the delivery of GRD’s service makes it necessary to ensure that these systems are developed, operated, used and maintained in a safe and secure fashion in addition to paper based records.

The increasing need to transmit information across networks of computers renders the data more vulnerable to accidental or deliberates unauthorised modification or disclosure.

Legal Requirements

Some aspects of information security are governed by legislation, the most notable U.K. Acts are:

- The Data Protection Act (1998)
- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)
- Regulation of Investigatory Powers Act (2000)
- Freedom of Information Act (2000)
- Human Rights Act (2000)

Purpose and Scope of the Policy

The purpose of security in any information system, computer installation or network is to preserve an appropriate level of the following:-

- Confidentiality the prevention of the unauthorised disclosure of information
- Integrity the prevention of the unauthorised amendment or deletion Information
- Availability the prevention of the unauthorised withholding of information or resources

The level of security required in a particular system will depend upon the risks associated with the system, the data held on the system and the working environment of the system. This policy applies to all information held in both manual and electronic form

Who is affected by the Policy

The Policy applies to all employee’s of the company. It also applies to members, contractors and visitors, not employed by the company but engaged to work with or who have access to company information.

Where the Policy Applies

The Policy applies to all locations from which company systems are accessed (including home use, or other remote use). Where there are links to enable non-company organisations (to have access to company information, the company must confirm that the security policies they operate meet our security requirements or the risk is understood and mitigated

Specific Security Policy Objectives

- To ensure employee’s have a proper awareness and concern for computer systems security and an adequate appreciation of their responsibility for information security.
- To ensure all contractors and their employees have a proper awareness and concern for the security of company information.
- To provide a framework giving guidance for the establishment of standards, procedures and computer facilities for implementing computer systems security.