SG CIVIL ENGINEERING LTD

Cyber Security Policy
2024 – 2025

Table of Contents

Section

1.0 Introduction

1.1 This document provides the overarching governance policy for the protection and security of SG Civil Engineering Ltd (the Company) where it is dependent upon its Information Technology (IT) systems for its normal day to day business activities.

1.2 It is therefore essential for the continued successful operation of the Company that the confidentiality, integrity and availability of its IT systems and data are maintained at a high level at all times.

1.3 To achieve this, the Cyber Security Policy has been introduced and every individual who uses IT equipment is expected to read it and ensure that its provisions are complied with.

1.4 Where individuals fail to follow the procedures stated in this policy it may lead to disciplinary or 'Red / Yellow' Card action, prosecution in addition to this it may also render the individual personally liable for the cost of replacing or reinstating damaged or corrupt equipment and data.

1.5 The policy will be reviewed periodically (at least annually) and all changes will be brought to the attention of all individuals who use IT Equipment as part of their everyday work within the Company.

2.0 Objectives

2.1 The main objectives of this policy are:

- to present the management approved requirements, control objectives and principles for overall Cyber Security.
- to define the structure and roles within the Company Cyber Security structure.
- to maintain confidence that the Company's Cyber Security governance meets the requirements of the law including the data protection regulations, the guidance on government use of cloud services and other compliances as required.

3.0 Scope

3.1 This Cyber Security Policy will apply to:

- all Company directors, management, workers, and contractors;
- all assets owned by the Company;
- information held or owned by the Company, any IT equipment and infrastructure used, and the physical environment in which the information and/or supporting IT is used;
- employees, subcontractors and contractors of other organisations who directly or indirectly support the Company during its works;

3.2 The Company systems in a hosted / cloud environment.

- Where access is to be granted to any third party (e.g. contractors) compliance with this policy must be agreed and documented. A copy of this policy document will be issued to all those noted above.

4.0 Security Organisation

4.1 Responsibilities - The Company has appointed Helen Gallagher as the IT Manager who is responsible for:

- assigning security roles and responsibilities as required;

- co-ordinating the implementation of the security policy across the Company;
- reviewing and if appropriate updating this Policy;
- reviewing, logging and monitoring security incidents;
- reviewing third party access and security arrangements;
- monitoring exposure to major threats to information assets;

4.2 The security of all hardware located on specific sites where the Company has offices located is the responsibility of the site manager / supervisor appointed by the Company.

4.3 The security of all other hardware, operating systems, PC application, networking, infrastructure and corporate software is the responsibility of the IT Manager.

5.0 Acquisition of Information Technology (IT)

5.1 All acquisitions of IT shall be in accordance with the Company Procurement Procedures and be co-ordinated by the IT Manager who shall obtain specialist advice if they consider it appropriate.

5.2 Site Specific acquisitions shall be agreed between the Operations Director and the IT Manager.

5.3 The IT Manager has authority to replace obsolete equipment in accordance with specific business requirements and can upgrade / replace office productivity tools and software within an agreed budget.

6.0 Security Information Advice

6.1 Specialist advice on information security is available from the IT Manager.

7.0 Security Incidents

7.1 All suspected and actual security incidents shall be reported immediately (by the quickest means) to the Main Office where the IT Manager will ensure each incident is recorded, investigated and corrective action implemented where appropriate.

7.2 A security incident shall mean:

- any event arising from negligence or deliberate default that has, or could have, resulted in loss or damage to the Company's IT systems or data;
- a compromise to the confidentiality, integrity or availability of IT systems or data;
- an action that is in breach of the security policy;
- any cyber security threat or incident.

7.3 Any security incident that may have the potential to lead to disciplinary or 'Red / Yellow' Card action will require the appropriate involvement and consultation with the Operations Director and HR Manager.

7.4 Any security incident which leads to loss or damage, or wilful abuse of the conditions of this policy may be cause for investigation and, where appropriate, formal action, in accordance with the Company's agreed disciplinary policy or the requirements within the 'Red / Yellow' Card.

8.0 Security of Third Party Access

8.1 Where there is a business need for third party access to IT facilities and information assets the security implications and requirements will be determined, and controls agreed with the IT Manager and third party.

8.2 All new systems will be assessed for risks from third party connections.

8.3 Arrangements involving third party access, e.g. Support engineers, consultants will be based on a formal contract or security agreement containing, or referring to, all of the necessary security conditions, including obtaining an indemnity in respect of any loss caused by erasure or alteration of data or incorrect alteration of programs.

8.4 In certain circumstances it may be necessary to divulge a password for access by technical support staff and in such cases, it must be changed immediately after the authorised activities are completed.

9.0 Assets Control

9.1 An inventory of IT assets shall be maintained by the IT Manager who shall promptly update it for all acquisitions, disposals, updates and management of the Company cyber assets (this includes transfer of assets to another user). The accuracy of the inventory shall be audited internally annual to ensure accuracy.

9.2 All users must notify the IT Manager if they move an asset to another location which is not their normal appointed place of work.

10.0 Personnel Security

10.1 All users are responsible for the equipment issued to them and information that they have access to. Third party access to IT equipment and data, without prior arrangement with the IT Manager is prohibited.

10.2 When accessing Company information, they must ensure that they do so in a secure environment and that persons who are not authorised to view said information cannot view it.

11.0 Equipment & Environmental Security

11.1 Equipment Security - IT equipment and cabling should be protected from spillage or leaks and must be sited away from where others have access e.g. (Site Offices) and also to minimise opportunities for unauthorised access or removal. All Managers / Supervisors (Users) should also be warned of the dangers of spilling liquids or food on IT equipment.

11.2 All Managers / Supervisors (Users) should always ensure that computer equipment and screens are positioned to prevent unauthorised viewing of data.

11.3 Any faulty IT equipment (Business owned) shall be reported to the IT Manager who will arrange for its repair or replacement. Under no circumstances shall anyone attempt to repair, move, change equipment or open casings except for printers to replace consumables or clear a paper jam.

11.4 Equipment & Data Destruction - Obsolete equipment shall be checked by the IT Manager and all hard disks will be thoroughly cleansed of data before disposal, whether by sale, donation or destruction.

11.5 Equipment will normally be disposed of via a third-party accredited data disposal organisation who will ensure recycling, where possible. Any PCs disposed of by sale / donation will not include the operating system installed and no application software.

11.6 All IT equipment will be disposed of in accordance with the relevant environmental legislation e.g. WEEE Directives.

12.0 Protection from Malicious & Unauthorised Software

12.1 It is essential that special measures are implemented to prevent the introduction of malicious software such as computer viruses, ransomware and malware or the use of unauthorised software.

12.2 Using unlicensed software can result in a fine, adverse publicity and a block on the use of any computers until the licences are paid for or the offending software is removed, resulting in very serious disruption to the Company's activities.

12.3 A computer virus or similar can cause severe damage to data and hence serious disruption. Every precaution must be taken to protect all Company data and programs.

12.4 Unauthorised software is software that has not been purchased by, or whose purchase or use has not been agreed by the IT Manager.

12.5 To reduce the risks of infection or use of unauthorised software the following preventive and corrective measures will be place:

- the introduction and/or use of unauthorised software, including screensavers, is prohibited and may lead to the application of relevant, formal disciplinary action;

- software licences will be complied with at all times;

- reputable, up to date anti-virus software must be installed and will be used to detect and remove or isolate viruses and malware. The IT Manager can advise on approved software;

- any suspected viruses must be reported immediately to the IT Manager and, where appropriate, logged as a security incident;

- except where there is a justifiable business reason that has been expressly agreed with the IT Manager, users should not open unsolicited e-mails from unverifiable sources and especially any attachments as there is a significant risk, they may contain a virus;

- users must not attempt to download executable files, i.e. program software, from the Internet without prior specific clearance from the IT Manager.

13.0 Electronic Mail

13.1 Controls to reduce the security risks associated with electronic mail (e-mail) should be implemented covering:

- vulnerability to unauthorised interception or modification. Confidential data should only be sent in encrypted form;

- vulnerability to error, for example incorrect addressing;

- publication of directory entries;

- remote access to e-mail accounts.

- Users shall avoid responding to unsolicited e-mails from unverifiable sources, and in particular, except where there is a justifiable business reason that has been expressly agreed with the IT Manager, shall not open such mail or any attachments in such circumstances as there is a significant risk they may contain a virus.

13.2 All e-mail inbound and outbound will be subject to security scans for spyware, malware and viruses.

14.0 Internet Use

14.1 The use of the Internet on the Company provided Wi-Fi shall be controlled to prevent:

- users wasting time by playing or "surfing" when they are paid to work;

- users accessing sites and importing material which the Company, as a matter of policy, may find unacceptable;

- users accessing sites and importing illegal material;

- users importing a virus or other malicious software and hence compromising the accuracy, availability and confidentiality of the Company systems;

14.2 Internet access is to be used only for access to sites relevant to work or vocational training during an individual's working hours.

15.0 User Responsibilities

15.1 To prevent unauthorised computer access effective security requires the co-operation of authorised users. Users must comply with Company policies, standards and procedures regarding access controls, in particular the use of passwords and the security of equipment.

15.2 In order to maintain security users must:

- not write passwords down where others may readily discover them;

- not tell anyone else their password;

- not use obvious passwords such as their name;

- not let other people observe when entering their password;

- use a password with at least eight characters in it including numeric or special characters;

- promptly change their password if they suspect anyone else may be aware of it;

- log out of applications if they will be away from their desk for any length of time;

- 'lock' their PC when away from their desk to prevent it being used by others;

- not to open e-mails containing suspicions attachments;

- check e-mail and names of people they received a message from to ensure they are legitimate;

- report scams, privacy breaches and hacking attempts;

S Gallagher
Operations Director
SG Civil Engineering Ltd

1st June 2024