Information Security Risk Policy Statement

Effective from 25th October 2022
Review date June 2023

MJ Gleeson PLC is committed to protecting its information systems and data which are critical business assets. The purpose of Information Security Risk Policy Statement is to protect all information assets and data. The policy statement includes technology and behaviour, training and awareness, communications and review.

Scope

The scope of this policy encompasses all forms of information security threats including, but not limited to, malware, emotet, DoS, SQLi, password attacks and phishing emails. It applies to all employees and assets.

Responsibilities & Review

The IT Director is responsible for identifying the resources required to ensure compliance with this Policy Statement. We pride ourselves on having an "open door" ethos and all staff are signposted to raise any concerns through the appropriate channels and process. Senior management review meetings are held with The Audit Committee being briefed on all information security risk matters at least 3 monthly. Reviews include, but are no limited to, breaches, attempted breaches, risks and opportunities and any changes in law or legislation which may impact the business.

Breach of Information Security and Systems

The Group has not been subjected to any Information Security breach within the last 3 years. Any breach or attempted breach would be investigated with any corrective actions and preventative measures being implemented.

Compliance Obligations

The Group meets its compliance obligations in relation to Information Security.

MJ Gleeson plc
6 Europa Court
Sheffield Business Park
Sheffield
S9 1XE

Information Security Risk Insurance

The Group maintains an established Information Security Risk insurance programme which is appropriate to the size, scale and context of the business and encompasses, data breach, loss of data and business continuity.

Training & Awareness

All employees are provided with mandatory training on information security matters including modules discussing cyber security and GDPR. This mandatory training is provided to all new starters and is an annual mandatory requirement.

Internal Policies and Procedures

To support this policy statement at operational level, our IT and Communications Systems Policy outlines the standards which must be observed when using our systems. It covers all employees, officers, consultants, contractors, volunteers, interns, casual workers, agency workers and anyone who has access to our IT and communication systems.

Communication of Policy Statement

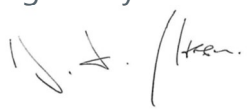
This policy is publicly available on our website and is always accessible to all colleagues through internal information systems.
Changes to this policy are communicated to all colleagues through bulletins and other appropriate communication methods.

Review of Policy Statement

This policy will be reviewed

- at least annually and / or;
- where there is a change in operation or scope which may impact this policy
- where there is a breach of this policy
- as a result of legislative changes

Signed by



Date 26th October 2022

MJ Gleeson plc
6 Europa Court
Sheffield Business Park
Sheffield
S9 1XE