INFORMATION SECURITY POLICY STATEMENT

INFORMATION SECURITY POLICY STATEMENT

Information is an important business asset, adds significant value to the company and needs to be protected from threats that could potentially disrupt business continuity. CWG has written information security policy based on ISO/IEC 27001:2022 standard to provide a mechanism that establish procedures to protect her information assets against security threats and to minimize the impact of security incidents.

The purpose of this information security policy is to protect the company's information assets from all threats, whether internal or external, deliberate, or accidental.

The Policy Scope covers Physical Security, IT Infrastructure Security and Environmental Security which encompasses all forms of Information Security such as data stored on computers, transmitted across networks, printed, or written on paper, sent by fax, stored on media or spoken in conversation or over the telephone.

All managers are directly responsible for implementing the Policy within their business areas, and for adherence by their staff.

It is the responsibility of each employee to adhere to the policy. Disciplinary processes will be applicable in those instances where staff fail to abide by this security policy.

ISMS objectives are:

- Achieve 100% compliance with CWG's legal, regulatory, and contractual obligations related to information security
- Improve CWG's incident response time by 90% through enhanced processes and regular training
- Implement protective measures to ensure 99.9% availability and integrity of information while maintaining strict confidentiality within CWG.
- Establish a pervasive culture of Information Security Management system integration across all CWG's operations and processes

The information security manager is responsible for maintaining the policy and providing support and advice during its implementation. The review of the Information Security Policy and related documents shall be performed on an annual basis or when significant changes occur to ensure suitability, adequacy, and effectiveness of the ISMS.

Approved by

Managing Director

Date: 22/08/23