Information Security Policy Statement

Revision	Change Description	Created by	Approved By	Date Created
1.0	Initial Issue	Jade Le Gray-Wise	Stuart Ladbrook	09/12/2020
1.1	Review	Jade Le Gray-Wise	Stuart Ladbrook	17/05/2024

This document is held as a controlled electronic file.

PRINTED COPIES ARE UNCONTROLLED and will not be updated.

1. Purpose

Onwave UK Limited ("the Company") has developed and maintains a Company Management System (CMS) covering all the Company's activities. An important element of this is the Information Security Management System (ISMS) section of the system which has been designed to comply with the requirements of ISO 27001.

The purpose of this document is to define the role that the Company **Board of Directors** and **Senior Management Team** (inclusive of **Department Leads**) take in the Information Security Management System (ISMS). This ensures the commitment to information security, the development and propagation of the information security policy, and the assignment of appropriate information security roles, responsibilities and authorities.

2. Scope

To define the Company's *Information Security Policy* and ensure the appropriate information security roles, responsibilities and authorities are assigned.

3. Roles and Responsibilities

Relevant roles and responsibilities with regard to information security and the ISMS are defined in *Master Document Register* and expanded upon within the CMS documentation. The roles and responsibilities for the *Information Security Policy* are as follows:

Document Owner: Security Officer

- The **Security Officer** shall be the *Information Security Policy* **Document Owner,** responsible for ensuring it is maintained, regularly reviewed and updated in line with the requirements of ISO 27001.
- Though the **Security Officer** is the **Document Owner,** changes to the policy must be discussed with the **Board of Directors**.
- Responsible for ensuring that roles, responsibilities and authorities are appropriately assigned, maintained and updated as necessary.

Board of Directors:

- Responsible for setting and approving the *Information Security Policy* with the **Security Officer**.

Quality Manager

- Responsible for supporting the **Security Officer** in the implementation and effective management of the ISMS.

Senior Management Team

- Responsible for ensuring the requirements of the information security policies and procedures are adhere to in their department and reporting breaches.

All Employees

- Responsible for adhering to the requirements of the Information Security Policy and for fulfilling any duties related to assigned roles, responsibilities or authorities.

Suppliers/subcontractors

- Responsible for adhering to the requirements of the *Information Security Policy* and for fulfilling any duties and expectations outline in the Interested Parties Log.

4. Policy Description

4.1. Commitment and Continuous Improvement

The Company *Information Security Policy* demonstrates the **Senior Management Teams** commitment to information security and the ISMS. This commitment extends to all processes and controls defined within the scope of the ISMS as well as legislative obligations. The *Information Security Policy* is developed in accordance with both clause 5.2 of ISO 27001 and Annex A control 5.1.

The **Senior Management Team** are committed to preserving the confidentiality, integrity, availability and privacy of all the physical and electronic information assets throughout the company in accordance with the scope defined in the *Context of the Organisation Procedure* in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image.

The ISMS is subject to continuous, systematic review and improvement in line with the *Internal Audit Procedure*.

The Company **Senior Management Team** including the **Security Officer**, **Department Leads** and other specialists support the ISMS framework and periodically review the security policy.

The Company is committed to achieving, and maintaining thereafter, certification of its ISMS to ISO 27001.

4.2. Context of the Organisation

Onwave provides a range of connectivity and digital technology solutions within several sectors including but not limited to: Construction, Infrastructure, Utilities, Public Sector, Transport and Highways.

The Company currently employs staff in a main office location: 4 Abbey Wood Road, Kings Hill, West Malling, Kent. However, staff also work remotely based on hybrid working arrangements which means they work from home or customer locations. Refer to the *B200 - Company Management System Manual v2.0*.

The Company's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS. The *Risk Register, Statement of Applicability and Risk and Opportunity Management Procedure* identify how information-related risks are controlled.

The Company aims to achieve specific, defined Information Security Objectives, which are developed in accordance with the business objectives, the context of the organisation, the results of risk assessments and the risk treatment plan. See the *CMS Objectives* record for the Information Security Objectives and the *Company Management System Manual* for further information.

All Employees of Onwave and external parties identified in the *Interested Parties Log* are expected to comply with this policy and with the CMS that implements this policy. All Employees and required external parties will receive and/or be required to provide appropriate training. The consequences of breaching the *Information Security Policy* are set out in the *Employee Handbook* and in contracts and agreements with third parties. Any observed or suspected security breaches are to be reported. This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

Stuart Ladbrook

Chief Executive Officer (CEO)

13/05/2024