1   INFORMATION SECURITY POLICY

1.1   Purpose

This policy is implemented to manage direction and support for information security in line with the organization's requirements, as well as accordance with relevant laws and regulations.

This Information Security Policy will to clarify and set conditions in order to establish and achieve information security objectives.

By implementing this Information Security Policy OWL will ensure continual improvement on its information security management system.

1.2   Scope

This document applies to all employees of OWL. In addition, it applies to personnel contracted by OWL to complete work on their behalf.

1.3   Policy

OWL shall:
- ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered;
- ensure that employees and contractors are aware of and fulfil their information security responsibilities during employment;
- ensure protection of the organization's interests as part of the process of changing and terminating employment;
- ensure to identify information assets in scope for the management system and define appropriate protection responsibilities;
- ensure that information receives an appropriate level of protection in accordance with its importance to the organization and relevant stakeholders;
- ensure users are authorized to access systems and services as well as prevent unauthorized access;
- ensure the protection of information in networks and its supporting information processing facilities;
- ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information;
- ensure correct and secure operations of information processing facilities;
- ensure that information and information processing facilities are protected against malware;
- ensure that information security is an integral part of information systems across the entire lifecycle;
- ensure the protection of data used for testing;
- ensure that an agreed level of information security and service delivery is maintained in line with supplier agreements;
- ensure a consistent and effective approach to the lifecycle of incidents, events and weaknesses;
- ensure compliance with all applicable legislation and contractual requirements;
- ensure that information security is implemented and operated in accordance with the organizational policies and procedure.

OWL will:

- maintain a management framework to initiate and control the implementation and operation of information security within the organization;
- maintain a management framework to ensure the security of teleworking and use of mobile devices;
- prevent unauthorized disclosure, modification, removal or destruction of information stored on media;
- limit access to information and information processing facilities;
- make users accountable for safeguarding their authentication information;
- prevent unauthorized access to systems and applications;
- prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities;
- prevent loss, damage, theft or compromise of assets and interruption to the organization's operations;
- record events and generate evidence to ensure the integrity of operational systems and to prevent exploitation of technical vulnerabilities;
- minimize the impact of audit activities on operational systems;
- maintain the security of information transferred within the organization and with relevant stakeholders;
- protect the organization's valuable assets that are accessible to or affected by suppliers;
- make sure to embed information security continuity in the organization's business continuity management systems.

Name	M.C. van der Giessen
Function	CEO
Date	01-02-2023
Signature	