

ISMS01	<b>FluidOne</b>	Issue: 5.0
Page 1 of 2	<b>Information Security Policy</b>	Date: 15/01/19

## 1 PURPOSE

It is FluidOne's policy to develop, implement and maintain an Information Security Management System that:

- Provides assurance within the company and to our clients and partners that the availability, integrity and confidentiality of their information will be maintained appropriately;
- Manages information security risks to all company and customer assets;
- Protects the company's ongoing ability to meet contracted commitments through appropriate Business Continuity;
- Bases information security decisions and investments on risk assessment of relevant assets considering; Integrity, Availability and Confidentiality;
- Takes into account business and legal or regulatory requirements, and contractual security obligations;
- Maintains awareness of all employees so they can identify and fulfil contractual, legislative and company specific security management responsibilities
- Minimises the business impact of and deals effectively with security incidents.

This Policy is supported by the following objectives:

- Implementation of a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001 Standard for Information Security Management Systems;
- Implementation of a sensitive Information Classification and Exchange Policy including compliance with regulations under the Data Protection Act 1998 to protect client, partner, supplier, our own and personal employee information which is not in the public domain;
- Implementation of an Information Security Risk Assessment Process that assesses the business harm likely to result from a security failure and the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and controls currently implemented;
- Development and implementation of a Business Continuity Plan to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters;
- Defined security controlled perimeters and access to controlled offices and facilities to prevent unauthorised access, damage and interference to business premises and information;
- Information security awareness guidance for all company employees;
- An ISMS Management Team that supports the continuous review and improvement of the company ISMS;
- Implementation of incident management and escalation procedures for reporting and investigation of security incidents for ISMS management review and action.

The FluidOne Information Security Policy is reviewed by the ISMS Management Team who recommend amendments and updates to the policy as part of the continuous service improvement process.

Document Owner: Chief Operating Officer  
*Printed copies are uncontrolled, verify current issue before use.*

**DOCUMENT CLASSIFICATION: UNCLASSIFIED**

ISMS01	<b>FluidOne</b>	Issue: 5.0
Page 2 of 2	<b>Information Security Policy</b>	Date: 15/01/19

## 2 APPLICABILITY

This document is applicable to all FluidOne staff and contractors.

Signed: \_\_\_\_\_

Russell Horton, CEO - FluidOne Ltd

Date: 15<sup>th</sup> January 2019

Review Date: 15<sup>th</sup> January 2020

## 3 CHANGE CONTROL

Version	Date	Status (i.e. Draft or Issue)	Summary Description of Change(s)	Approver (Job Title)
0.1	26/02/14	First Draft	New Document	JB
0.2	17/02/14	Second Draft	Minor changes following discussion at IS/ BC Forum	JB
1.0	17/04/14	Issue	First Issue	CR
2.0	11/12/15	Issue	Second Issue	PW
3.0	11/12/16	Issue	Updated for FluidOne	PW
4.0	11/12/17	Issue	Reviewed for CEO endorsement	PW
5.0	15/01/19	Issue	CEO updated and general policy refresh	PW

Document Owner: Chief Operating Officer  
 Printed copies are uncontrolled, verify current issue before use.

**DOCUMENT CLASSIFICATION: UNCLASSIFIED**