Comply Flow Pty Ltd
L2, 34 Belgrave St
Manly NSW 2095

COMPLYFLOW
ABN: 92 137 044 494
ACN: 137 044 494

Information Security Policy

Version	Approved by	Approval date	Effective date	Next review date
1.1	Managing Director	1 November 2019	1 November 2019	1 November 2020

Table of Contents

1. Purpose, Scope & Users

The purpose of this policy document is to set out the principles, objectives and components of Comply Flow's Information Security policies, procedures and management system. The policy sets out management's information security direction and is the backbone of Comply Flow's Information Security Management System (ISMS), which establishes the framework for ongoing management and continuous improvement of our resilience to information security threats.

Users of this document include Comply Flow employees, users, delivery partners and external parties who are interested in the principles, policies and procedures which underpin our commitment to information security.

1.1 Reference Documents

ISO 27001: 2013 standard; clauses 5.2, 5.3

2. Principles & Objectives

Comply Flow is committed to preserving the confidentiality, availability and integrity of information and information systems which are central to our company purpose in providing a secure service for clients and users, and as an employer.

Comply Flow information - whether processed directly by Comply Flow or managed by third parties - is an important asset that must be protected. Improper use of information resources may result in harm to Comply Flow and our users, clients and staff.

This commitment to the protection of information assets forms the foundation of our Information Security Management System (ISMS). Comply Flow Management accept responsibility for establishing and maintaining the ISMS and ensuring that sufficient that sufficient resources are allocated to fulfil its objectives. Importantly, Comply Flow is committed to the continuous improvement of the ISMS in order to safeguard the organisation's resilience to evolving information security threats.

2.2 Information Security Terminology

Confidentiality		characteristic of the information by which it is available only to authorized persons or systems
Integrity		characteristic of the information by which it is changed only by authorized persons or systems in an allowed way
Availability		characteristic of the information by which it can be accessed by authorized persons when it is needed
Information Security		preservation of confidentiality, integrity and availability of information
Information Security Management System		part of overall management processes that takes care of planning, implementing, maintaining, reviewing, and improving the information security

3. Scope

The Information Security Management System is based on the ISO27001: 2013 international standard.

The scope of the certified Information Security Management System is for:

'The protection of all information and data assets for the delivery of all of Comply Flow's organisational functions, services and activities. These include all business processes, including where external third-party suppliers are engaged, involved in the provision of Comply Flow's commercial services.'

For further details regarding the Scope of the ISMS, please send a request to:

support@complyflow.com.au

4. Policy Framework

As part of implementing the ISMS, Comply Flow reviewed and consolidated our policy framework for information security, in addition to integrating requirements of the ISO27001: 2013 standard with our existing policy documentation.

5.1 Policies

5.1.1 IT Security Policy

Our IT Security Policy (CF-POL-20190601-IT Security Policy) sets out rules for the acceptable use of information systems and other Comply Flow assets. Its sections cover IT Acceptable Use, Information Classification, Secure Disposal & Destruction and Information Transfer.

5.1.2 Data Security & Backup Policy

Our Data Security & Backup Policy (CF-POL-20190601-Data Security & Backup Policy) outlines the key technical principles and requirements for the development, use and management of Comply Flow information systems and other information assets, in order to preserve their confidentiality, integrity and availability for all users and parties covered in the ISMS scope. Its sections cover Data Security, Cryptographic Controls, Change Management, Secure Development & Maintenance, Information Backup, Logging & Monitoring, Technical Vulnerability Management and Network Controls.

5.1.3 User Access Control Policy

Our User Access Control Policy (CF-POL-20910601-User Access Control Policy) establishes our company framework for providing and maintaining secure access to information systems, for all employees, clients, system users, delivery partners and other third parties. Its sections cover Principles of Access Control, User Access Provisioning & De-Provisioning, User Obligations, Information Access Restrictions, Secure Logon, Password Management System and Privileged Utility Management.

5.1.4 Supplier Security Policy

Our Supplier Security Policy (CF-POL-20190601-Supplier Security Policy) sets out our company principles for managing third party risk, and defines clear rules for Comply Flow's relationship with

suppliers and delivery partners. It covers Relationship with Suppliers & Partners, Contracts, Access Rights, Ongoing Third Party Risk Management and Supplier Training & Awareness.

5.1.5 Privacy Policy

Our Privacy Policy (CF-POL-20190601-Privacy Policy) establishes our company commitment to, and principles for, protecting confidential information and data.

6. Procedures Framework

Our company ISMS is structured according to the following critical information security procedures, which are continually reviewed and consolidated with the aim of building continuous improvement into our processes through adoption of key controls from ISO/IEC 27001: 2013.

6.1 Procedures

6.1.1 Secure Development Procedures

Our Secure Development Procedures (CF-PRO-20190601-Secure Development Procedures) outline the key requirements and processes for secure development of software and information systems in order to safeguard the integrity, confidentiality and availability of information assets and systems. This document covers Data Security, Cryptographic Controls & Key Management, Change Management, Backup, Network Security Management, Information Transfer and System Monitoring.

6.1.2 Incident Management Procedure

Our Incident Management Procedure (CF-PRO-20190601-Incident Management Procedure) sets out the key processes to be followed to ensure quick detection of security events and weaknesses, and appropriate reaction and response to security incidents. It covers Receipt & Classification of Incidents, Treatment Process, Learning From Incidents and Disciplinary Action.

6.1.3 Business Continuity & Disaster Recovery Plan

Our Disaster Recovery Plan (CF-PRO-20190601-Business Continuity & Disaster Recovery Plan) covers the critical disaster scenarios or disruption events which fundamentally threaten business continuity and Comply Flow information assets. It defines clearly and precisely the action steps necessary to securely recover IT infrastructure and services, including critical databases and information. Its sections cover General Information, Personnel and Authorisations, Key Contacts and the Disaster Recovery Process for several critical scenarios.

6.1.4 Access Management Manual

Our Access Management Manual (CF-PRO-20190601-Access Management Manual) outlines the key components of user access for both Comply Flow staff and our cloud-service customers, which aim to preserve the confidentiality, integrity and availability of information assets and systems. It sets out principles for managing Role-based access control (RBAC) procedures, and covers Employee Onboarding, Managing Privileged Access, Revoking Staff Access & Password Management.

6.1.5 Employment Procedure

Our Employment Procedure (CF-PRO-20190601-Employment Procedure) outlines steps that Comply Flow managers must take when setting up new employees with accounts, and granting access to Comply Flow information systems. It covers Commencement of Employment (Screening Processes, Documentation, Legal, Training and Access), Induction Training, Developer Onboarding, Role Changes and Termination of Employment.

7. Legislative & Prudential Framework

Our Information Security Management System was developed in consideration of the following legislative and prudential requirements:

- *Privacy Act 1988*
- *The Information Privacy Act 2014 (ACT)*
- *Privacy and Personal Information Protection Act 1998 (NSW)*
- *Information Act (NT)*
- *Information Privacy Act 2009 (QLD)*
- *Information and Protection Act 2004 (TAS)*
- *Privacy and Data Protection Act 2014 (VIC)*
- *Health Records Information Privacy Act 2002 (HRIP Act)*

- *The Protective Security Policy Framework (Attorney-General's Department)*
- *Prudential Standard CPS232 Business Continuity Management (APRA)*
- *Prudential Practice Guide CPG 234 Management of Security Risk in Information and Information Technology*

Endorsed by

Mitchell Bourne
Managing Director

1st November 2019

If you have any questions regarding our Information Security Policy, please do not hesitate to reach out by contacting:

support@complyflow.com.au