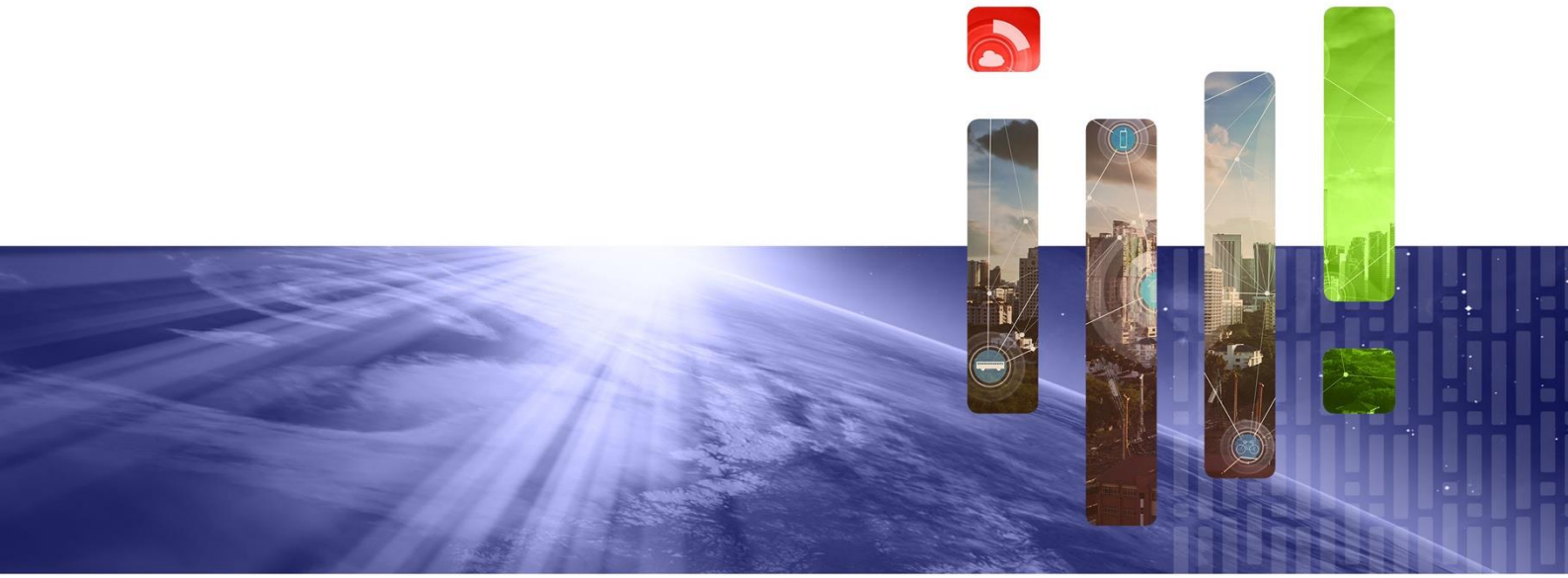
resillion

Quality and Information Security Policy

REFERENCE	ISO9001:2015, ISO27001:2022
DOC NUMBER	01-IMS-002
VERSION	v2.0
DATE	06 December 2023
STATUS	Approved
APPROVED BY	Yaron Kottler
AUTHOR	Teresa Cheung
CLASSIFICATION	Public



Distribution	
Name	Organisation
Public	Any

Revision Record				
Date	Version	Amendment	Author	Review
2023-02-10	0.1	First Draft	Teresa Cheung	
2023-02-11	0.2	Interim Review	Peter Burge	
2023-04-20	0.3	Include references, merged with DFIR security policy and update on Forensic Code	Teresa Cheung	
2023-05-01	0.4	Interim Review	Dan Martland	
2023-05-16	0.5	Resolve review comments	Teresa Cheung	
2023-06-19	0.6	Change to Resillion word template	Teresa Cheung	
2023-06-20	0.7	Final review	-	Atiquah Vohra
2023-06-21	1.0	Approval	-	Dik Vos
2023-12-06	2.0	Update CEO Approval	Teresa Cheung	Yaron Kottler

Contents

1 Quality and Information Security Policy

Resillion Senior Leadership team is committed to maintaining an Integrated Management System (IMS) in accordance with ISO9001:2015 and ISO27001:2022, placing high priority on customer focus, satisfying applicable statutory, regulatory and contractual requirements, and seeking for continual improvement. The IMS includes the Quality Management System (QMS) and the Information Security Management System (ISMS).

Resillion aims to be the "Guardians of the Connected World" and achieve the following:

- To deliver high quality technology and service-based solutions to our customers that are fundamental to their digital transformation goals.
- Our customers and potential customers will regard us as thought leaders for quality and security assurance across the world.
- To ensure we have the highest levels of customer engagement by understanding our customer's business goals.
- To be a preferred employer through providing a rewarding, challenging and supportive work environment.

Resillion is also committed to ensuring that the "confidentiality", "integrity" and "availability" of our information and IT assets are protected against:

- Unplanned downtime or outages;
- Accidental or malicious exposure, interference or damage; and
- Unauthorized access.

The approach to security will enable and not detract from working transparently and openly, and delivering services efficiently and effectively.

Resillion continually monitors and improves the effectiveness of its IMS through the use of:

- Policies and procedures
- Security controls
- Quality objectives which are set and reviewed annually
- Analysis of data including risk assessment and treatment
- External and internal audit results
- Corrective and improvement actions, and
- Management review.

An induction programme is provided to all new staff to cover the awareness to IMS and to embed the right security culture. Technical training is provided for all service and product delivery staff. All staff are required to work in accordance with the documented policies and procedures in all aspects of their roles. All personnel are made aware of the relevance and importance of their activities and how they contribute to the achievement of the objectives of the IMS.

A Global QA Manager, CISO & Privacy Officer, Teresa Cheung, is appointed and has the overall responsibility for all aspects of the IMS.

We continually strive to ensure the highest standards of integrity are applied to all our activities worldwide in accordance with international best practices. For any feedback, please contact hello@resillion.com.

Signed by:

Yaron Kottler

Executive Chairman and Interim CEO, Resillion

06 December 2023

2 References

[1] ISO9001:2015 Cl. 5.2

[2] ISO27001:2022 Cl. 5.2

[3] ISO27002:2022 Cl. 5.1

[4] Forensic Codes of Practice and Conduct Issue 7 (and Code of Practice Version 1 2023) Cl. 23.3 (and 32.3)