



INFORMATION SECURITY POLICY

QF 41



+353 1 211 9900



www.evcoms.com



info@evcoms.com





Contents

Contents.....	2
1. PURPOSE	4
2. SCOPE.....	4
3. RESPONSIBILITY.....	4
4. DEFINITIONS	4
5. RELATED DOCUMENTS	4
6. INFORMATION SECURITY OBJECTIVES.....	5
7. INFORMATION SECURITY RESPONSIBILITIES	5
8. RISK ASSESSMENT AND TREATMENT.....	5
9. INFORMATION SECURITY CONTROLS.....	5
10. COMPLIANCE AND AUDITING	6
11. INCIDENT RESPONSE	6
12. SECURITY AWARENESS AND TRAINING	6
13. CONTINUOUS IMPROVEMENT	6

Document Control

Title	QF 41 Information Security Policy
Version	2.0

Current Revision

	Written / Revised By	Reviewed and Approved for and on behalf of evcoms by
Name	Emily Francis	Brian Fitzpatrick
Title	OpEx Specialist	CSO
Signature		
Signature Date	30/11/2023	01/12/2023
Effective Date	01/12/2023	

Revision History

Version	Date	Issued By	Status	Comments
1.1	08/05/2018	Mark Evans	Draft of New evcoms Data Encryption Policy	
1.2	25/05//2018	Mark Evans	Document released	
1.3	16/05/2019	Hiba Fadil	Document Reviewed and tested	
1.4	06/07/2023	Emily Francis	Sensitivity info added	
2.0	30/11/2023	Emily Francis	Released	Updated as per Eoghan Kenny

Document Classification

evcoms has classified this document as stated in the header. We do not wish for any third party other than that specifically tasked with its evaluation to have access to any content.

This document may contain sensitive information, which if were to be obtained by a competitor could place evcoms at a disadvantage.

We hope you look upon this statement favourably.

1. PURPOSE

evcoms is committed to maintaining the highest standards of information security to safeguard our valuable assets, ensure the confidentiality, integrity, and availability of information, and protect the interests of our clients, partners, employees, and stakeholders. This Information Security Policy outlines our commitment to ISO 27001 standards and serves as the foundation for our Information Security Management System (ISMS).

Our commitment to information security reflects our dedication to maintaining the trust of our clients, partners, and stakeholders. By adhering to this policy, we ensure the ongoing protection of our information assets and the sustainability of our business operations.

This security information policy will cover key principles that evcoms has in relation to maintaining and adhering to the security of its company information, employee information, customer information and all technology and communication systems.

2. SCOPE

This policy applies to all employees, contractors, third-party vendors, and stakeholders who access, process, store, or manage company information assets. It encompasses all aspects of information processing, storage, transmission, and disposal within our organisation.

The Scope of our ISMS is the: "Provision of managed services, strategic technical consultancy and support services across a wide range of products."

3. RESPONSIBILITY

It is the responsibility of the COO to ensure this policy is implemented and maintained across the organisation.

It is the responsibility of the wider management team and supervisors to ensure this policy is adhered to within their local teams.

It is the responsibility of all company employees and contractors to be aware of their obligations under this policy and to raise awareness of risks and opportunities associated with it.

4. DEFINITIONS

N/A

5. RELATED DOCUMENTS

[QF 101 Encryption Policy.docx](#)

[QF 41 Information Security Policy.docx](#)

[QF 89 Acceptable Use of Assets Policy.docx](#)

[QF 89 Access Control Policy.docx](#)

[QF 90 Supplier Security Policy](#)

[QF 95 Physical and Environmental Security Policy](#)

6. INFORMATION SECURITY OBJECTIVES

Our information security objectives are set, reviewed and monitored regularly.

The ISMS and the objectives are designed to:

- a. Ensure the confidentiality, integrity, and availability of information assets.
- b. Identify and assess information security risks regularly.
- c. Implement appropriate controls to mitigate identified risks.
- d. Continuously improve our information security management system.
- e. Foster a culture of security awareness and responsibility among all personnel.

7. INFORMATION SECURITY RESPONSIBILITIES

Senior Management: Our leadership is committed to providing the necessary resources, support, and direction to maintain an effective ISMS that complies with ISO 27001.

Information Security Management Team: The appointed ISMS Team is responsible for overseeing the implementation, maintenance, and continuous improvement of the ISMS.

Employees: All personnel are responsible for adhering to security policies, reporting security incidents, and actively participating in security awareness and training initiatives.

8. RISK ASSESSMENT AND TREATMENT

We undertake a systematic approach to identifying, assessing, and managing information security risks in accordance with ISO 27001. This includes:

- a. Identifying information assets and associated risks.
- b. Evaluating the impact and likelihood of identified risks.
- c. Implementing controls to mitigate or reduce risks to an acceptable level.
- d. Regularly reviewing and updating risk assessments as necessary.

9. INFORMATION SECURITY CONTROLS

We implement a comprehensive set of information security controls based on ISO 27001 Annex A, customised to our organisation's needs, and added to as deemed appropriate.

10. COMPLIANCE AND AUDITING

We commit to conducting regular internal audits and reviews of our ISMS to ensure compliance with ISO 27001 requirements. We also engage in external audits to validate our information security practices and seek certification as evidence of our commitment.

11. INCIDENT RESPONSE

In the event of a security incident or breach, we have established procedures to effectively respond, mitigate, and recover. This includes reporting incidents promptly, assessing impact, notifying relevant stakeholders, and implementing corrective actions.

12. SECURITY AWARENESS AND TRAINING

We recognise that information security is a shared responsibility. All personnel receive appropriate training and awareness programs to ensure they understand their roles in safeguarding information assets and adhering to security policies.

13. CONTINUOUS IMPROVEMENT

We are dedicated to continually improving our ISMS based on regular reviews, lessons learned from incidents, and changes in the threat landscape. We encourage all employees to provide feedback and suggestions to enhance our information security practices.