Document **[PPCDSFDSOP013]**	Title: **Information Security Awareness, Education and Training**	
Revision **1.0**	Prepared By: **Mark Anthony Bezzina**	Date Prepared: **11.03.2022**
Effective Date: **28.03.2022**	Approved By: **Jonathan Vassallo**	Date Approved: **28.03.2022**

Purpose: The purpose of this document is to provide guidance on information security awareness, education, and training, in order to facilitate the compliance with Key Requirement 6 of the *Checklist for the Commission and Member States on a common methodology for the assessment of management and control systems in the Member States*, sub-item 6.3.a. The Managing Authority follows ISO/IEC 27001:2017 and ISO/IEC 27002:2017 standards and controls.

Scope: This document highlights the information security awareness, education and training; hereinafter referred to as information security programme, being organised within the Managing Authority. Stakeholders may have other programmes that compliment this information security programme.

Background: Information security protects information from unauthorised activities, including access, modification, recording, disruption, and deletion. The goal is to ensure the safety and privacy of information.

Responsibilities:

- Head Managing Authority
- Chief Coordinators
- Heads of key stakeholder organisations
- Project Leaders
- All stakeholders

Procedure:

1.0 INTRODUCTION

1.1 All employees of the Managing Authority should receive appropriate awareness, education and/or training and regular updates in organisational policies and procedures, as relevant for their job function.[1]

1.2 Stakeholders' employees should also receive appropriate awareness, education and/or training and regular updates in organisational policies and procedures, as set by the respective organisation.

1.3 Where relevant, stakeholders may also receive additional appropriate awareness, education and/or training related to procedures set by the Managing Authority. Any such programme would not be a replacement of the stakeholder organisation's programme but an additional to the programme provided by the respective organisation.

2.0 IMPLEMENTATION GUIDANCE

2.1 The information security awareness programme should aim to make employees, and where relevant stakeholders, aware of their responsibilities for information security and the means by which those responsibilities are discharged.

2.2 The information security awareness programme takes into consideration the Government of Malta's information security policies and relevant procedures[2], taking into consideration the organisation's information to be protected and controls that have been implemented to protect the information.

2.3 The awareness programme should be planned taking into consideration the employee's role in the organisation, and where relevant, the organisation's expectation of the awareness of the external stakeholders.

2.4 The activities in the awareness programme should be scheduled over time, so that the activities are repeated and cover new employees and, where relevant, stakeholders.

2.5 Awareness training can use different delivery methods including noticeboard notifications, emails, online learning, and classroom-based training.

2.6 Information security education and training should also cover general aspects such as:

[1] ISO/IEC 27002:2017 control 7.2.2

[2] Government of Malta Information Security Policy available at https://mita.gov.mt/portfolio/ict-policy-and-strategy/gmict-policies/

a. stating Government of Malta's commitment to information security throughout the organisation;

b. the need to become familiar with and comply with applicable information security rules and obligations, as defined in policies, standards, laws, regulations, contracts and agreements;

c. personal accountability for one's own actions and inactions, and general responsibilities towards security or protecting information belonging to the organisation and external parties;

d. basic information security procedures (such as information security incident reporting) and baseline controls (such as password security, malware controls and clear desks); and

e. contact points and resources for additional information and advice on information security matters including further information security education and training materials.

2.7 Initial education and training will be provided to those who join the organisation, or transfer to new positions with substantially different information security requirements.

2.8 The awareness programme should not only focus on the 'what' and 'how', but also the 'why'. It is important that the target audience understands the aim of information security and the potential impact, positive and negative, on the organisation of their own behaviour.

2.9 An assessment of the training attendees' understanding will be conducted at the end of an awareness, education and training course to test knowledge transfer.

3.0 IMPLEMENTATION PROGRAMME

3.1 The information security awareness education and training progamme will be carried out using a variety of channels:

a. Security-related emails provided by Malta Information Technology Agency (MITA) in their role as Government of Malta's IT Agency and service provider to the Managing Authority;

b. Security-related emails sent by the Office of the Chief Information Officer responsible for EU Funds;

c. Information uploaded from time to time on the Structural Funds Database 2014-2020;

d. Training provided by the Institute for the Public Service, https://publicservice.gov.mt/;

e. Other awareness, education and training programmes as approved by the Head of the Managing Authority.

3.2 Employees of the Managing Authority are expected to attend a training course / seminar on information security of at least 3 hours on an biennial basis. A certificate of attendance is to be obtained by the employee, and the unit responsible for training should be informed.

3.3 Should any employee be unable to attend the training organised by the Managing Authority, they should make their own arrangements to attend a similar training programme and inform the unit responsible for training.

Revision History:

Revision	Date	Description of changes	Requested By
1.0	28.03.2022	Circulated final version	DG PPCD