NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

EG|CERT

MALWARE PROTECTION AND THREAT INTELLIGENCE POLICY

V1.0

TLP: WHITE

THE TRAFFIC LIGHT PROTOCOL (TLP)

The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s).
The protocol includes four colors (traffic lights), which are detailed as follows:

Red- Not for disclosure, restricted to participants only:
Sources may use TLP:RED when information cannot be effectively acted upon by additional parties. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed

Amber- Limited disclosure, restricted to participants' organizations:
Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

Green- Limited disclosure, restricted to the community:
Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

White- Disclosure is not limited:
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. TLP:WHITE information may be distributed without restriction.

TABLE OF CONTENTS

POLICY REVISION HISTORY

AUTHOR	DESCRIPTION	VERSION	DATE
(EG-CERT)	RELEASE DATE	1.0	
(EG-CERT)	EFFECTIVE DATE	1.0	
	REVIEW DATE		
	REVISION DATE		

SIGN-OFF

SIGN-OFF LEVEL	DATE	NAME	SIGNATURE
Top management			
Executives			
Security Director			
IT Director			
Internal Audit Team Director			

1. POLICY OVERVIEW

This policy establishes "the Organization's Malware Protection and Threat Intelligence Policy" that aims to implement protection processes and procedures against malware to protect the organization's assets, collect and analyze the information related to information security threats and attacks "threat intelligence".

1.1 PURPOSE

The Egyptian Computer Emergency Readiness Team (EG-CERT) has developed this Policy that helps organizations to provides protection against malware and raises awareness about its threat environment so that the appropriate mitigation actions can be taken.

1.2 SCOPE

This Policy applies to all information technology assets and resources in the organization. All parties dealing with the organization are responsible for complying with this policy.

1.3 MANAGEMENT COMMITMENT

IT and Security Directors have reviewed and approved this Policy and the Top Management supports the purpose thereof. Disciplinary action may be taken against any employee violating this Policy; this might include the suspension of the violating employee, restrictions on his access to some systems or information, or more severe penalty, including, but not limited to, the employee's termination.

1.4 COMPLIANCE WITH INTERNATIONAL STANDARDS

This Policy has been set based on NIST Special Publication (SP) 800-53 (Rev. 5), ISO 27001, and complies as well with ISO 27002 Best Practices for Information Security.

2. POLICY DEFINITIONS

DEFENSE-IN-DEPTH:

Refers to the multi-level security defense through different security controls at the level of people, technology and operational processes.

BUSINESS CONTINUITY PLAN:

Refers to the documentation of a predetermined set of instructions or procedures that describe how to attain the sustainability and continuity of the organization's performance of its mission/ business processes during and after the occurrence of a major service outage or disruption.

THREAT INTELLIGENCE:

Refers to information about cyber threats and risks that have been aggregated, analyzed, interpreted, or verified to provide the suitable context and basis for the decision-making process.

3. ROLES AND RESPONSIBILITIES

Stakeholder	Responsibilities
Top Management	• Approves and officially endorses this Policy. • Issues administrative instructions that are binding on all organization's employees to implement the policies, and set the regulation of disciplinary penalties related to the employee's failure to implement these policies, in a manner that does not conflict with the applicable regulations and laws.
Executives	• Reviews and officially endorses this Policy.
Security Team	• Sets security plans, procedures, policies and measures in collaboration with the IT Department. • Reviews and updates this policy periodically. • Implements and reviews the mechanisms needed to endorse this Policy. • Maintains the security and protection of systems and data. • Manages, updates and follows up on the tools that maintain system and data security. • Collaborates with IT and Internal Audit Teams to secure the organization's digital assets. • Rejects or approves any necessary exceptions to this Policy.
HR Team	• Ensures that all employees are aware of the organization's security policies. • Specifies the information security responsibilities and confidentiality clauses in contracts.
IT Team	• Collaborates with the Security Team to issue the plans, procedures and measures needed for the implementation of this policy. • Informs all organization's employees of their security duties and responsibilities before giving them access to sensitive data and systems. • Implements the necessary mechanisms requested by the Security Team.

Stakeholder	Responsibilities
Internal Audit Team	• Carries out an internal audit of the security controls of the policy and its efficiency. • Assesses and consolidates the organization's readiness for encountering any cyberattacks. • Assesses and manages risks. • Ensures the compliance with policies and standards.
Managers	• Ensures that the employees concerned are familiar with this policy.
Employees	• Employees must implement this policy and act in accordance therewith.

4. MALWARE PROTECTION AND THREAT INTELLIGENCE POLICY CONTROLS

4.1 PROTECTION AGAINST MALWARE

- Computers and electronic storage media should be checked and scanned with anti-malware periodically.
- All downloaded files, applications and any data must be checked and scanned with an anti-malware.
- The use of any unauthorized software must be prevented by using techniques such as “the Application Allow-List”.
- The visiting of harmful websites should be detected and prevented by using appropriate techniques such as “Black-listed websites”.
- The vulnerability management procedures should be implemented.
- The usage of the Defense-In-Depth Approach must be taken into consideration.
- The business and operational continuity plans should be developed to ensure the organization’s recovery from malware attacks. These plans should include taking data backups, recovering data and keeping an offline backup.
- The malware protection procedures should be determined; this includes the provision of training on the implementation of such procedures.
- The appropriate channels should be established to alert about and report any malicious code detected.
- Spam protection mechanisms should be used to protect against malicious emails.
- All employees must be trained on how to identify malware and mitigate their potential impacts.
- The employees must keep abreast of all advancements and developments in the field of malware and how to encounter and prevent them.

4.2 THREAT INTELLIGENCE

- Threat intelligence about existing or emerging threats should be monitored, aggregated and analyzed.
- Threat intelligence should be relevant and related to the scope of the organization's activities and digital assets.
- Threat intelligence should provide an accurate insight into the threat landscape for each organization.
- The organization should take appropriate actions based on threat intelligence quickly and effectively.
- The needed sources of the information should be determined and monitored in order to issue cyber threat reports.
- It is required to communicate with competent employees, and inform them of threat intelligence, that should be in a form and format that is intelligible, apprehensible and can be easily handled.
- The information aggregated from threat intelligence sources should be added to information security risk management processes as additional feeds for the malware prevention and detection controls.
- It must be ensured that all threat intelligence is not circulated outside the organization except after the obtainment of a prior permission from the top management, whether through the employees or via cyber security solutions.

4.3 POLICY EXCEPTIONS

The security team must be informed of any proposed changes to be made to the system; the endorsement of any exception to the fundamental controls principles stipulated in this Policy must be documented and formally approved by the IT Director. Policy exceptions must determine:

- The nature of the exception;
- A realistic clarification of the necessity of the Policy exception;
- Any risks ensuing from the Policy exception;
- Evidence of the IT Director's approval of this exception.