Information Classification Policy
V1.0. – 06 June 2015 (Draft).

Number of Pages: 4

Classification: TLP: WHITE. **Owner: AfricaCERT.**

Introduction.

Classification of information is essential to a CSIRT. Without classification everyone treats the same piece of information differently, which could have major consequences. Therefore, to get everyone on the same page, a policy is needed.

The AfricaCERT Information Classification Policy is based on the Traffic Light Protocol (TLP) used widely by the international CSIRT community. (1).

(1) https://www.trusted-introducer.org/ISTLPv11.pdf

1. The Principles

All AfricaCERT members share in the responsibility for ensuring that information assets receive an appropriate level of protection by observing this Information Classification policy. AfricaCERT Teams follow and honor the TLP (Traffic Light Protocol); protocol recognized, supported and widely accepted in the CSIRT Community.

Information 'owners' shall be responsible for assigning classifications to information assets according to AfricaCERT information classification policy presented below. Where practicable, the information category shall be embedded in the information itself.

AfricaCERT Members shall be guided by the information category in their security-related handling of information. If TLP is not supported by the external entity, the classification schemes of both entities must be matched in order to guarantee information confidentiality.

2. TLP Classification

The TLP classification comprises the following rules; all communications, are tagged in the subject as TLP:Colour where Colour is RED, AMBER, GREEN or WHITE.

A similar stamp should be clearly visible on the cover and in the footer of all documents sent to or issued by AfricaCERT. If contact is
By phone or videoconference, the TLP classifications are stated prior to the delivery of the information.

Table: TLP Classification

TLP colour	Rules to be applied
RED	Non-disclosable information, restricted exclusively to representatives actually participating in the information exchange. Representatives must not disseminate the information outside the exchange. RED information may be discussed during an exchange, if all the representatives participating subscribe to these rules. Guests and others such as visiting speakers who are not full members of the exchange will be required to leave before such information is discussed.
AMBER	Limited disclosure, restricted to members of the information exchange, people within their organisations and/or constituencies (whether direct employees, consultants, contractors or out-source staff working for the organisation) who need to know in order to take action.
GREEN	Information may be shared with other organisations, information exchanges or individuals in the network security, information assurance or CNI community at large, but not published or posted on the web.
WHITE	Information that is for public, unrestricted dissemination, publication, web-posting or broadcasting. Any member of the information exchange may publish the information, subject to copyright. Confidential and internal classified information must not be disclosed using the white colour.

2. Email and Written Information

For information exchange by email or in written form, AfricaCERT adds an additional Data Security Mechanism.

TLP Color	Data Security Mechanism
RED	Data securing mechanism: Encrypted and signed (if possible)
AMBER	Data securing mechanism: Encrypted and signed (if possible)
GREEN	Data securing mechanism: signed (if possible)
WHITE	Information can be shared publicly in accordance with the law

3. Chatham House Rule (CHR) in addition to TLP

AfricaCERT extends the Traffic Light Protocol with a specific tag called Chatham House Rule (CHR). When this specific CHR tag is mentioned, the attribution (the source of information) must not be disclosed. This additional rule is at the discretion of the initial sender who can decide to apply or not the CHR tag. As an example, Chatham House Rule can be used when a reporter of a security vulnerability don't want to be disclosed.

4. Default Classification

Any information received from an AfricaCERT member by another APCERT member that is not classified in accordance with the TLP must be treated as AMBER, unless otherwise advised in writing by the AfricaCERT member that owns /disseminated the information,

5. TLP Example.

The table below provides an example of TLP usage.

TLP Color	Description	Examples
RED	Information exclusively and directly given to (a group of) individual recipients. Sharing outside is not legitimate	People in a meeting, direct message (1-to-1, strictly limited)
AMBER	Information exclusively given to an organization; sharing limited within the organization to be effectively acted upon	CSIRTs sending indicators of compromise to an organization (1-to-group, limited)
GREEN	Information given to a community or a group of organizations at large. The information cannot be publicly released.	CSIRTs sending a specific security notification to a sector (1-to-many, limited)
WHITE	Information can be shared publicly in accordance with the law	Public security advisory or notification published on the Internet (1-to-any, unlimited)

The TLP AMBER classification can be expressed in the following way

TLP:AMBER

If you need to extend the classification with the Chatham House Rule

TLP:AMBER TLP:EX:CHR

If you have different TLP classifications in the same document, you must clearly express the classification at each line.

TLP:AMBER ……
TLP:GREEN …….

Additional Credits:
CERT.LU - https://www.circl.lu/pub/traffic-light-protocol/
APCERT -http://www.apcert.org/documents/pdf/APCERT_Information_Classification_Policy.pdf
ENISA - https://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/policies/basic-policies-1/information-disclosure-policy