Information Sharing and Handling Policy

V4.0. – Updated August 21, 2022

Number of Pages: 5

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

(1). https://www.first.org/tlp/.

1. The Principles.

AfricaCERT members must adhere to AfricaCERT's policy on Information Sharing and Handling. Trust and confidence are vital when sharing information. Appropriately assigning TLP designations and handling information builds and maintains trust and confidence within the AfricaCERT community and strengthens cooperative and collaborative efforts to prevent and mitigate malicious cyber activity.

All AfricaCERT members share the responsibility for ensuring that information assets receive an appropriate level of protection by observing this Information Sharing and Handling 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 an external entity, the classification schemes of both entities must be matched in order to guarantee information confidentiality.

2. TLP Classification.

Table: TLP Classification

FIRST TRAFFIC LIGHT PROTOCOL (TLP) Version 2.0	TLP: CLEAR	TLP: GREEN	TLP: AMBER	TLP: AMBER+STRICT	TLP: RED
May be shared with those with a need-to-know within a formal organization of which the recipient is a member (company, ISAC, …)	✓	✓	✓	✓	✗
May be shared with those with a need-to-know in organizations to which the recipient provides cybersecurity services	✓	✓	✓	✗	✗
May be shared with members of wider security community	✓	✓	✗	✗	✗
May be shared without limits	✓	✗	✗	✗	✗

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

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.

3. 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 required)
AMBER	Data securing mechanism: Encrypted and signed (if required)
GREEN	Data securing mechanism: signed (if possible)
CLEAR	Information can be shared publicly.

4. 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 doesn't want to be known.

5. Default Classification

Any information received from an AfricaCERT member by another AfricaCERT 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.

6. TLP Example.

The table below provides an example of TLP usage.

TLP Color	Description	Examples
RED	Information is 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 send 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)
CLEAR	Information can be shared publicly	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

When required to extend the classification with the Chatham House Rule
TLP:AMBER: EX:CHR

When required to have different TLP classifications in the same document, you must clearly express the classification at each line.
TLP:AMBER ……
TLP:GREEN …….

Additional Credits:

APCERT - Information Sharing Policy (AfricaCERT as APCERT Strategic Partner; AfricaCERT members follow APCERT Information Sharing Policy when exchanging information with APCERT members.
FIRST – TLP 2.0
FIRST - Information Exchange Policy (IEP)

Document Revision

V.1. 06 June 2015
V.2. 18 December 2018 (updated link to TLP; title changed).
V.3. 03 October 2019. Updated Additional Credits section.
V.4. 21 August 2022. Updated with TLP 2.0