Information handling and Classification

* Rarenet supports the Information Sharing Traffic Light Protocol (https://www.first.org/tlp/)

Data classification description

PUBLIC
This information is deemed to be non-sensitive and can be distributed to anyone in any context. Meaning the information excludes personal data and details on digital emergencies, mitigation strategies, escalations and internal procedures, or other details that could lead to identifying users at risk or other individuals involved in the rapid response processes. The information is intended for public consumption. It may have already been reported on, and/or is available to be reported on.

CONFIDENTIAL
Information marked as confidential can be shared to all members of [rarenet]. If not indicated otherwise, any information circulated on [rarenet 112] mailing lists and other platforms will be considered confidential to members of that group. There should be no assumption about sharing the information to third parties, and this kind of information should only be shared on a need-to-know basis with third parties that have signed a non-disclosure agreement. Confidential information is deemed to be sensitive because it includes details about digital emergencies, mitigation strategies, escalations and internal procedures developed inside [rarenet].

RESTRICTED
Information that includes personal identifiable information or details that can lead to the identification of users at risk or individuals involved in the rapid response process should not be shared withing the RRN public lists but restricted to groups or individuals on a need-to-know basis.

Information Protection
Public information can be widely distributed and takes the form of newsletters, website content, social media posts, etc.

Confidential information is stored in platforms that are only accessible by the [rarenet] members that have been mandated by their networks/communities to manage these platforms.

Members of Rarenet hold themselves accountable for the loss, seized or detected compromises of their devices holding confidential data. The expectation is to inform as soon as possible the Rarenet members and to detail what protections were in place and active as of the time of loss or seizure (e.g. powered off, encrypted volume dismounted, or taken while fully logged in, etc.)

Retention Policy
All information in the [rarenet 112] infrastructure, except for public information which is non-sensitive and does not include any personal data, is stored on password-protected platforms requiring 2-factor authentication, and in work devices with full-disk encryption.

In case of a personal data breach which is likely to result in a risk to the rights and freedoms of the data subjects, [rarenet mailing lists and website] administrators shall notify the data subjects without undue

delay, no later than 72 hours after having become aware of the breach, in accordance with the EU's General Data Protection Regulation. In addressing data security breaches, [rarenet mailing lists and website] administrators shall take measures to mitigate damage, investigate, conduct remedial action and comply with regulatory requirements for information security.