Statement of the ICANN African community participating in the joint AFRALO–AfrICANN meeting in Dakar on 26 October 2011

The members of the ICANN African community participating in the joint AFRALO – AfrICANN meeting held on Wednesday 26 October 2011 in Dakar, during the 42nd ICANN international public meeting, having debated the dangers faced by the African Internet end-users due to the various forms of the cyber-criminality:

1. Exhort the African ccTLDs operators to implementation of DNSSEC as a crucial measure to secure DNS

2. Encourage the African counties to create operational authorities of certification using public keys (electronic signature).

3. Recommend that all Africain end-users to use the electronic signature to encode or sign the electronic messages with confidential or critical content.

4. Encourage the African countries that do not have yet a Computer Emergency Response Team (CERT) to create one to respond in a timely manner to the requests of the Internet users and provide them with the necessary advice based on updated security information

5. Recommend the establishment of a Public Private Partnership initiative to develop guidelines for children protection against child abusive material on Internet. The initiative should adapt the global draft child on line protection guidelines published by the ITU to individual country's environment and push for policy and legal framework to implement the guidelines that should address the responsibilities of the stakeholders ie ICT Industry, Policy, Legal and Law Enforcement Agencies, Parents, Teachers and Guardians, and then the Children and Youth.

6. Advise the African parents to equip their systems with parental control software, while mentoring their children and making them aware of the threads on the net

7. Invite all the African Internet users to contact their national Computer Emergency Response Team (CERT) to learn about the latest virus alerts, and follow its advice to avoid any damage to their systems.

8. Encourage the update of the various declarations and African positions on Cybercrime, involving the Internet end-users and the civil society in the process.

9. Invite the African countries to cooperate for a better harmonization and an update of the legal framework dealing with the Cyberspace.

10. Encourage the organization of formation programs for instructors about issues of Internet Security and cyber-criminality.

11. Recommend to the African users of the Internet to follow closely the minimum safety rules listed below:
    - **Use good quality passwords**, that is to say difficult to find using automated tools and difficult to guess by a third party
    - **Have an updated operating system and software: browser, antivirus, office, personal firewall, etc…** because most attacks attempt to use the computer holes (holes of the operating system or of software)
    - **Perform regular backups** in order to be able to react to an attack or a malfunction.
    - **Disable by default ActiveX and JavaScript components**; although they allow many interesting functions, they present in the meantime security risks up to the takeover of the control of a vulnerable machine by an intruder
    - **Do not hurry in clicking on links**, but take the URL yourself and put it in the browser address bar, as a standard attack consists in encouraging Internet users to click on a link in a message to mislead him and steal his/her personal information.
    - **Dissemination of personal information:** A good practice consists in never give personal information in forums, and never enter personal and sensitive data (such as bank information) on sites that do not offer all required guarantees
    - **Never pass on hoaxes** such as letters chain, lucky winner, financial pyramid, call for solidarity, virus alert, etc…
    - **Cultivate prudence**: Internet is a street full of unknown people, and generally, it is recommended to not automatically trust the sender's name that appears in the message, and never meet with a stranger without a minimum precaution.
    - **Vigilance before opening attachments to an e-mail**: they often peddle malware