RENU Joins MANRS

KAMPALA – Thursday, 15th October 2020

On Tuesday 13th, October, 2020, RENU joined Mutually Agreed Norms for Routing Security (MANRS). MANRS is a global initiative aimed at greatly improving the security and resilience of the Internet's global routing system. It does this by encouraging those running Border Gateway Protocol (BGP) to implement well-established industry best practices and technological solutions that can address the most common threats.

RENU chose to join this initiative in order to improve its security posture on the Internet from routing incidents that have for a longtime caused network outage, data losses and cost implications to many victims on the internet.

Such incidents include, route hijacks where an attacker announces network prefixes on Internet belonging to another network as if those prefixes were theirs; route leaks where an organization accidentally propagates routing announcement(s) beyond their intended scope; and IP Spoofing where false Internet Protocol (IP) packets are created with a false source IP address for the purpose of impersonating another device or host.

To be become a member of MANRS, RENU had to be tested against the following criteria:

Filtering – preventing propagation of incorrect routing information so that organizations announce To adjacent networks the Autonomous System (AS) numbers and IP prefixes they or their customers are legitimately authorized to originate.

Anti-spoofing – preventing traffic with spoofed source IP addresses by implementing a system that enables source address validation for their own infrastructure and end users, and for any Single-Homed Stub Customer Networks.

Coordination – facilitating global operational communication and coordination between network operators where organizations must ensure that up-to-date contact information is entered and maintained in the appropriate Regional Internet Registry (RIR) database and/or in PeeringDB.

Global Validation – facilitating validation of routing information on a global scale where organizations must either have a publicly documented routing policy that includes all AS numbers and IP prefixes they advertise to other networks or must have created valid Route Origination Authorizations (ROAs) for all IP prefixes or sets of prefixes they are legitimately authorized to originate.

Having fulfilled all the requirements, RENU was duly accepted to be part of the great initiative that promotes best practices against most threats. RENU is the first network in Uganda to join MANRS, demonstrating our strong commitment towards ensuring that education and research institutions in Uganda operate in secure cyber space.

Join the RENU network, and work securely online.