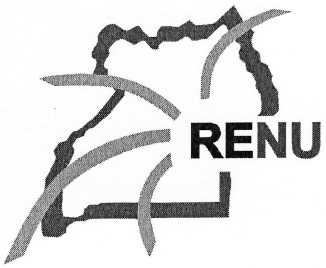

Enabling Research & Education Collaboration

RENU-CERT

Description

Version 3.0

This document is written in accordance to RFC 2350 <https://www.ietf.org/rfc/rfc2350.txt>

TABLE OF CONTENTS

1. About This Document 3
2. Contact Information 4
3. Charter 6
4. Policies 9
5. Services 11
6. Incident Reporting Forms 13
7. Disclaimers 13
8. REFERENCES 14

N.H

1. About This Document

The RENU-CERT Description document states and explains the RENU constituency's expectations of the RENU-CERT, how it can be contacted, the services it provides and level of support it can offer, among others.

This document is also meant to guide the RENU-CERT in their daily engagements with RENU Secretariat staff, RENU member institutions, and other stakeholders.

The document shall be periodically reviewed for it to remain relevant to the changing needs and expectations of the RENU constituency.

Signature of RENU Head of Department, Systems and Software

Sign: _____ **Date:** 09/02/2024

Signature and stamp of RENU Chief Executive Officer

Sign: _____ **Date:** 09/02/2024

Stamp:

RESEARCH & EDUCATION NETWORK FOR UGANDA
RENU
09 FEB 2024
HOUSE NO. 31, THE EDGE
MAKERERE UNIVERSITY

1.1. Locations Where This Document Maybe Found

The current version of this CSIRT description document is available from the RENU-CERT website here: https://cert.renu.ac.ug/files/renu-cert--description-v3.pdf. Please make sure you are using the **latest** version.

1.2. Authenticating This Document

The **English** version of this document has been signed with the RENU-CERT's PGP key. The signature is also on the RENU-CERT website, under: https://cert.renu.ac.ug/files/renu-cert--description-v3.asc.

2. Contact Information

2.1. Name Of The Team

Short name: RENU-CERT

Full name: the Research and Education Network for Uganda - Computer Emergency Response Team

2.2. Address

Location 1:

House No.31 | The Edge

Makerere University - Main Campus

P. O. Box 35009, Kampala

Uganda

Google Maps Link: https://goo.gl/maps/8qh4jT8ak2PzDkRJ9

Coordinates: 0.3318715301075764, 32.56864523729965

Location 2:

Rashida Towers

Plot 6B, Mabua Road, Kololo

Kampala, UGANDA

Google Maps Link: https://goo.gl/maps/AHRxcP6GNNEmi9JJ9

Coordinates: 0.33276900143006616, 32.58850423729973

2.3. Time Zone

Eastern Africa Time (EAT) +0300 UTC/GMT

N.H

2.4. Telephone Number

RENU NOC phone number: +256-783-979-515

RENU Systems department phone number: +256-783-619-776

NB: When you call, ask for a team member on-duty from the RENU-CERT or explain the issue to the RENU NOC or RENU Systems department personnel and they will escalate it to the RENU-CERT.

2.5. Electronic Mail Address

cert@renu.ac.ug

This is a **group** email address that relays email to the entire RENU-CERT.

2.6. Public Keys And Other Encryption Information

The RENU-CERT has a OpenPGP key with the details below:

Key Fingerprint: `C5EA 4C0E 90F6 DFB1 0531 1F90 E55D AF0A 2BC0 253B`

Key ID: `0xE55DAF0A2BC0253B`

The key can be found on the RENU-CERT website at https://cert.renu.ac.ug/pgp/renu-cert--public-pgp-key.asc .

2.7. Team Members

All members of the RENU-CERT are listed on the RENU-CERT website, at https://cert.renu.ac.ug/cert-team.html.

2.8. Other Information

General information about the RENU-CERT, as well as links to various recommended security resources, can be found at https://cert.renu.ac.ug.

2.9. Points Of Customer Contact

The preferred method for contacting the RENU-CERT is via e-mail at <cert@renu.ac.ug>; e-mail sent to this address will notify the RENU-CERT member on-duty, or be forwarded to the appropriate backup person. If you require urgent assistance, please call the phone number indicated in the Telephone Number section.

If it is not possible (or not advisable for security reasons) to use e-mail, the RENU-CERT can be reached by telephone during regular business hours. Telephone messages (SMS) are checked less often than e-mail.

If possible, when submitting a report or feedback, use the forms mentioned in the Incident Reporting Forms section.

N.H

2.10. Working Hours

Monday – Friday, 08:00 hrs – 17:00 hrs, EAT

NB: Monday – Friday are considered to be working days, Ugandan and International public holidays excluded. List of Ugandan Public holidays can be found here: https://www.yellow.ug/public-holidays. For emergencies outside working hours, the RENU-CERT can be contacted through the RENU-NOC (Email: noc@renu.ac.ug , Telephone number: +256-783-979-515)

3. Charter

3.1. Mission Statement

The purpose of the RENU-CERT is to provide a secure environment for collaboration among Uganda's research and education institutions, as well as provide an effective and efficient response to their computer security incidents.

3.2. Constituency

The RENU-CERT's constituency is a **bounded** constituency, comprising the **entire** RENU community. This is further broken down into two sub-constituencies:

- **RENU Member Institutions** - all institutions/entities connected to or served by the Research and Education Network for Uganda (RENU).
- **RENU Secretariat** - the entire staff/team that run the operations of the Research and Education Network for Uganda (RENU).

In this document, phrases like "entire RENU constituency" or simply "RENU" refer to **both** sub-constituencies mentioned above, unless otherwise stated. For the sake for simplicity, the two groups will henceforth be collectively called "RENU". When specifying one sub-constituency, it will be stated explicitly as done above.

Because the RENU-CERT serves Ugandan academic institutions/entities connected to RENU, a national research and education network (NREN), it is fully defined as **an academic network CERT**.

3.3. Sponsorship And/Or Affiliation

The RENU-CERT is a sub-section of the RENU Technical team at the RENU Secretariat, and its reporting structure is as shown in Figure 1. It is affliated with:

- the sectorial CERT; UgCERT (under the Uganda Communications Commission, UCC) https://ug-cert.ug/
- the national CERT; CERT.UG/CC (under NITA-U) https://cert.ug/
- AfricaCERT; https://www.africacert.org/about-us/

Figure 2 shows the mentioned affiliations.

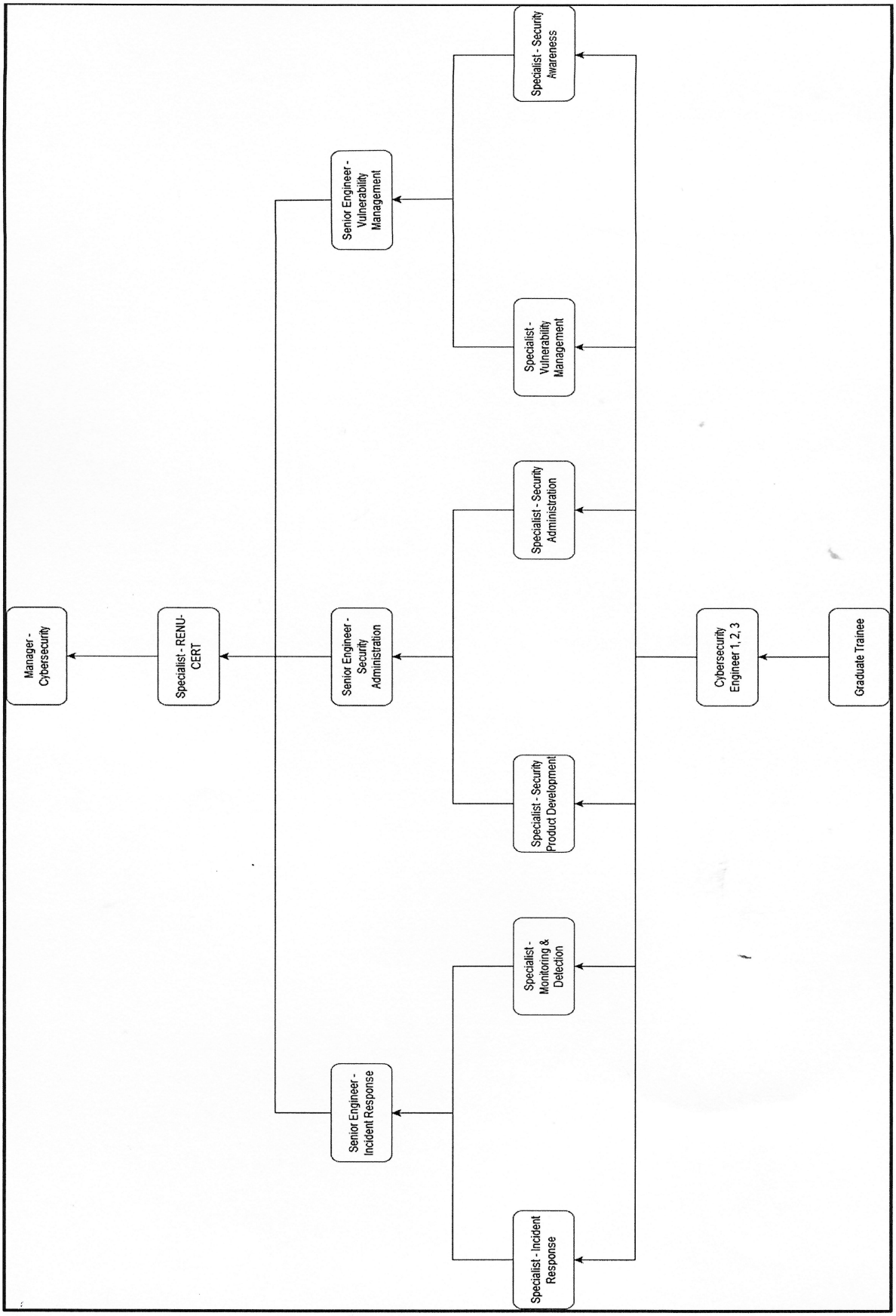

Figure 1: RENU-CERT Reporting Structure

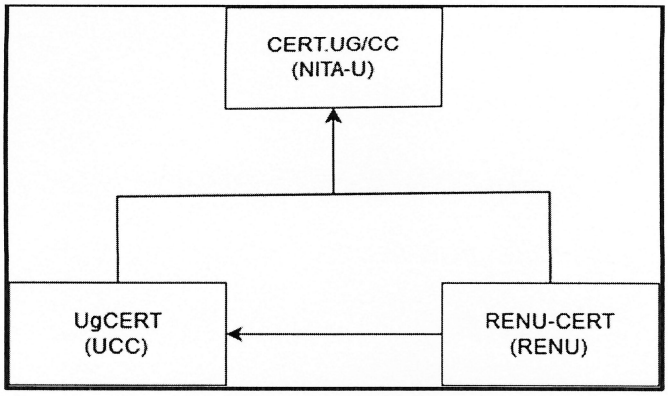

Figure 2: RENU-CERT Affiliations

3.4. Authority

The RENU-CERT has **shared authority** over the RENU constituency and **no authority** elsewhere. This means the RENU-CERT can make operational recommendations regarding vulnerabilities and mitigation of incidents and/or incident handling, and influence constituents to disconnect all or parts of their network until the incident has been resolved.

Additionally, it might **assist** the constituency by helping with coordination and response to the incidents, but the implementation of the recommendations **is not** the responsibility of the RENU-CERT, but **solely** of those to whom such recommendations are made.

As the need may arise from time to time to mitigate incidents in the RENU constituency, the RENU-CERT has the authority to:

- Perform RENU constituency network traffic filtering or blocking
- Install software agents on RENU Secretariat devices and systems to protect them from harm or misuse
- Deploy hardware devices in RENU Secretariat sites and Points of Presence (PoPs) to monitor and/or filter traffic as required
- Run non service-affecting vulnerability scans or other similar assessments on constituency IT infrastructure that use RENU public IP addresses.

3.5. Operated Network Numbers

The RENU-CERT operates the following public IPv4 networks:

- 196.43.128.0/18
- 137.63.128.0/17
- 102.34.0.0/16

The RENU-CERT operates on the following IPv6 networks:

- 2c0f:f6d0::/32

The RENU-CERT is assigned to the autonomous system of the Research and Education Network for Uganda (RENU); **AS327687**.

More information on this can be found here:

- https://bgp.he.net/AS327687
- https://www.peeringdb.com/net/11098

4. Policies

4.1. Types Of Incidents And Level Of Support

The level of support given by the RENU-CERT will vary depends on the Criticality Level, Incident Class and Reporting Time of incoming incident reports. The incidents the RENU-CERT can offer support on are categorised under multiple classes and tags. Each incident may be classified under one class and tagged with multiple incident tags.

The classes of incidents the RENU-CERT handles for the RENU member institution sub-constituency are in Table 1:

Table 1: Incident Classification

CLASS	ATTACKER	VICTIM
Inbound	Not in AS327687	In AS327687
Outbound	In AS327687	Not in AS327687
Intranet 1	In AS327687	In AS327687
Intranet 2	In RENU Member institution LAN	In RENU Member institution LAN

The tags of incidents the RENU-CERT handles for the RENU Member Institution sub-constituency are:

- (Distributed) Denial of Service
- Malware
- Email
- Policy Violation
- Other

Types of incidents other than those mentioned above will be prioritized according to their apparent severity and extent. The severity is termed as the Criticality Level and the details of the level of support offered by the RENU-CERT are as in Table 2:

Table 2: Incident Level Of Support

CRITICALITY LEVEL	MAXIMUM INCIDENT RESOLUTION TIME	EXPECTED LEVEL OF SUPPORT
Level 1 - Incident affecting **CRITICAL** systems or information with potential to be **revenue- or customer-impacting**.	Within 12 hours	• Email (and Phone call) communication • On-site support and coordination
Level 2 - Incident affecting **NON**-critical systems or information, **NOT** revenue- or customer impacting. Other investigations that are **time-sensitive** can be classified here.	Within 2 working days	• Email (and Phone call) communication • Remote support (but with possibility of hybrid i.e. remote & on-site) and coordination

Level 3 - **Possible** incident, **NON**-critical systems or information affected, **NOT** revenue- or customer impacting. Other investigations that are **NOT** time-sensitive. Long-term investigations involving extensive work can also be classified here.	Not time-bound	• (Optional) Email communication • (Optional) Remote support & coordination

For incidents that occur outside the bounds of the RENU constituency, technologically or otherwise, but request response from the RENU-CERT, the types of incidents to handle and level of support offered shall be determined on a case-by-case basis.

For more information, visit https://cert.renu.ac.ug/files/renu-cert--incident-handling-service.pdf.

4.2. Reporting Security Vulnerabilities As Part Of Research

In conformance with the RFC 9116 (https://datatracker.ietf.org/doc/html/rfc9116), cybersecurity researchers in the RENU constituency or on the general Internet may share information with the RENU-CERT through the information advertised in the **security.txt** file located on the RENU and RENU-CERT websites here:

- https://cert.renu.ac.ug/.well-known/security.txt
- https://renu.ac.ug/.well-known/security.txt

The RENU-CERT policy on this kind of outreach from the researcher community is as follows:

- **All** communication should be **encrypted**. The OpenPGP key for the RENU-CERT is as in the Public Keys And Other Encryption Information section. Since this might be two-way communication, the researcher(s) **MUST** avail their public OpenPGP key(s).
- The researcher(s) shall provide **valid identification** from their **home institution/organisation** to confirm identity, prior to further engagement. Failure to provide identification shall halt any further interactions.
- Appreciation and credit to the researchers for any vulnerabilities found shall be announced on the RENU Twitter channel (@renu_cert). The Traffic Light Protocol (https://www.first.org/tlp/) shall apply.

4.3. Co-operation, Interaction And Disclosure Of Information

Constituents' information will be availed to the RENU-CERT via a report form, (See Incident Reporting Forms section), and typically contains sensitive information such as IP addresses and personal contact information, and therefore must be securely transferred to the RENU-CERT.

To aid in investigations and response, some information from the constituent provided in the report might need to be disclosed to other involved parties or other CSIRTs. Therefore, a disclaimer on exactly what information will be disclosed will be included along with the report form.

N·H

The information to disclose might include:

- Incident tracking number
- Incident class and tag(s)
- Criticality level

Other information will only be disclosed on a **need-to-know** basis depending on the situation and authorisation from the reporter of the incident. The RENU-CERT shall use the Traffic Light Protocol (https://www.first.org/tlp/) when executing this redaction.

4.4. Communication And Authentication

In view of the types of information that the RENU-CERT will likely be dealing with, telephones will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted for transmission.

Where it is necessary to establish trust, for example before relying on information given to the RENU-CERT, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable degree of trust. Within RENU, and with known neighbour sites, referrals from known trusted people will suffice to identify someone. Otherwise, appropriate methods will be used, such as a search of FIRST members, the use of WHOIS and other Internet registration information, etc, along with telephone call-back or e-mail mail-back to ensure that the party is not an impostor. Incoming e-mail whose data must be trusted will be checked with the originator personally, or by means of digital signatures (OpenPGP in particular is supported).

5. Services

Visit https://cert.renu.ac.ug/cert-services.html for more information.

5.1. Reactive Services

These services are triggered by an event or request, such as a report of a compromised host, wide-spreading malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system. Reactive services are the core component of RENU-CERT work.

Reactive services are designed to respond to requests for assistance, reports of incidents from the RENU-CERT constituency, and any threats or attacks against constituent systems. Some services may be initiated by third-party notification or by viewing monitoring or intrusion detection system (IDS) logs and alerts.

5.1.1. Incident Handling

This is the RENU-CERT's **first and most important** service it renders to RENU. Incident handling involves receiving, triaging, and responding to requests and reports, and analysing incidents and events.

H.H

Particular response activities MAY include:

- taking action to protect systems and networks affected or threatened by intruder activity
- providing solutions and mitigation strategies from relevant advisories or alerts
- looking for intruder activity on other parts of the network
- filtering network traffic
- developing other response or workaround strategies

Visit https://cert.renu.ac.ug/files/renu-cert--incident-handling-service.pdf for more information.

5.1.2. Security-related Information Dissemination

This service provides RENU with a comprehensive and easy-to-find collection of useful information that aids in improving security. Such information might include:

- reporting guidelines and contact information for the RENU-CERT
- archives of alerts, warnings, and other announcements
- documentation about current best practices
- general computer security guidance
- vendor links
- other information that can improve overall security practices

This information is developed and published by the RENU-CERT, and can include information from external resources such as other CSIRTs, vendors, and security experts. This service includes maintaining a public or private archive or knowledge base of vulnerability, artefact or other incident information and corresponding response strategies.

Visit https://cert.renu.ac.ug/files/renu-cert--security-related-information-dissemination-service.pdf for more information.

5.2. Proactive Services

Proactive services are designed to improve the infrastructure and security processes of the RENU constituency before any incident or event occurs or is detected. The main goals are to avoid incidents and to reduce their impact and scope when they do occur.

5.2.1. Security Auditing And Assessments

This service provides a detailed review and analysis of a constituent's security infrastructure, based on the requirements they define or by other industry standards that apply. It may also involve a review of the constituent's security practices. There are currently two types of audits or assessments that the RENU-CERT provides. These are:

- **Vulnerability Scanning**—using vulnerability or virus scanners to determine which systems and networks are vulnerable, and provide possible remediation strategies.
- **Penetration Testing**—testing the security of a site by purposefully attacking its systems and networks.

M.H

Obtaining upper management approval is **REQUIRED** before conducting **penetration testing**, since some of the activities involved MAY be prohibited by the constituent's organisational policy.

Visit https://cert.renu.ac.ug/files/renu-cert--security-auditing-and-assessment-service.pdf for more information.

5.2.2. Filtering Services

This service involves filtering harmful traffic sent over various applications and protocols, used by RENU constituency. The aim of the service is to enhance the overall security posture of the RENU community, ensuring that students and staff of the RENU community are protected from malicious sites, while optimising bandwidth utilisation. Contact <cert@renu.ac.ug> for more information.

6. Incident Reporting Forms

The RENU-CERT provides multiple ways to report incidents.

- **Telephone and Email**: see Telephone Number and Electronic Mail Address sections.
- **RENU Support Helpdesk system**: Visit https://helpdesk.renu.ac.ug and raise a ticket with "Report a Problem / Cybersecurity Incident" as the help topic.
- **Offline Reporting Forms**: Find the appropriate incident reporting form via the RENU-CERT website, https://cert.renu.ac.ug, under "Support > Offline Form". Once filled in, please send them to <cert@renu.ac.ug> email address.

7. Disclaimers

- While every precaution will be taken in the preparation of information, notifications and alerts, RENU-CERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.

8. REFERENCES

1. RFC 2350 <https://www.ietf.org/rfc/rfc2350.txt>
2. CSIRT Description for SWITCH-CERT <https://www.switch.ch/security/.galleries/files/SWITCH-CERT.txt>
3. SIM3 Model & References <https://opencsirt.org/csirt-maturity/sim3-and-references/>
4. Security Vulnerability Disclosure <https://www.rfc-editor.org/rfc/rfc9116>