GARNET
Ghanaian Academic and Research Network

# COMPUTER SECURITY INCIDENT RESPONSE TEAM CHARTER


**GARNET CSIRT**

*Ghanaian Academic and Research Network*


**VERSION 1.0**

csirt.garnet.edu.gh

# Document Control

This charter is a controlled document. All revisions are recorded in the table below. The current version supersedes all previous versions. The authoritative copy is published at csirt.garnet.edu.gh.

## Revision History

| Version | Date | Author / Owner | Summary of Changes |
|---|---|---|---|
| 1.0 | 3 August 2026 | Emmanuel Togo, CTO | Initial approved release of the GARNET CSIRT Charter. |

## Approval

| Role | Name | Date Approved |
|---|---|---|
| Approved by (CEO) | Lucas Yikimpa Chigabatia | 14/09/2026 |
| Owner (CSIRT Coordinator) | Emmanuel Togo | |

# Authorization

This charter establishes the Ghanaian Academic and Research Network Computer Security Incident Response Team (GARNET CSIRT) to promote and enhance a safe cyber-ecosystem for GARNET's member institutions and the wider Ghanaian research and education community. The team is authorised to create and implement programs, policies, and initiatives that align with GARNET's strategic goals.

The GARNET CSIRT reports directly to the Chief Executive Officer (CEO) of GARNET. The Chief Technology Officer (CTO) is designated as the GARNET CSIRT Lead/Coordinator and is authorised to lead the team and coordinate its activities.

**Lucas Yikimpa Chigabatia**

(Chief Executive Officer)

Sign .....

**Emmanuel Togo**

(Chief Technology Officer / GARNET CSIRT Coordinator)

Sign .....

# 1. Introduction

The Ghanaian Academic and Research Network Computer Security Incident Response Team (GARNET CSIRT) is established to safeguard the cyber-ecosystem of Ghana's research and education community.

GARNET CSIRT operates as the coordinating CSIRT for GARNET's member institutions, providing incident coordination, threat intelligence sharing, and capacity-building support to member institutions' own security teams and IT staff. GARNET CSIRT does not replace or exercise operational authority over any member institution's internal security function; each institution retains full responsibility for its own incident response. GARNET CSIRT's role is to coordinate, notify, and support across the membership, and to serve as the trusted point of escalation between member institutions and regional/national bodies.

# 2. Scope

## 2.1. Publishing CSIRT Policies and Procedures

The policies and procedures related to GARNET CSIRT are enshrined in this document. Additional information for our constituents is published at https://csirt.garnet.edu.gh. GARNET CSIRT services are provided to member institutions of GARNET.

## 2.2. Relationships between different CSIRTs

CSIRTs do not work in isolation. GARNET CSIRT works with member-institution CSIRTs and security teams, as well as with regional and national bodies including the West and Central African Research and Education Network (WACREN) and Ghana's Cybersecurity Authority (CSA).

GARNET CSIRT operates as the coordinating CSIRT for Ghana's research and education community, facilitating information sharing and incident escalation between member-institution CSIRTs/security teams and regional or national bodies. GARNET does not exercise operational authority over member institutions' internal security functions but serves as a trusted point of coordination, notification, and capacity building for membership.

## 2.3. Establishing Secure Communications

For effective and secure communication with our constituents, to ensure data Confidentiality, Integrity and Authenticity, GARNET CSIRT shall work through channels including email and telephone. All correspondence is logged and tracked through GARNET's incident ticketing system to ensure accountability and continuity of response.

# 3. Information, Policies and Procedures

## 3.1 About this document

### 3.1.1 Date of Last Update: 3 August 2026

This is version 1.0.

### 3.1.2 Distribution List for Notifications:

Notifications of updates to this document are submitted via csirt@garnet.edu.gh. Subscription requests should be sent to the same address with the subject "mailing list subscription".

### 3.1.3 Locations where this Document May Be Found:

The current version of this document is available at csirt.garnet.edu.gh.

### 3.1.4 Authenticating this Document

The latest version of this document is signed with the GARNET CSIRT PGP key (fingerprint 684C 7B7D A77E 4F1B 68AE D3EC E84B 541C 6184 CC6F). The signature is available alongside this document at csirt.garnet.edu.gh.

## 3.2 Contact Information

### 3.2.1 Name of the CSIRT

"GARNET CSIRT": Ghanaian Academic and Research Network Computer Security Incident Response Team

### 3.2.2Mailing (Physical) Address

GARNET CSIRT
Ghanaian Academic and Research Network (GARNET)
VCG Office Complex, 6 IPS Road
Digital Address: GA-546-7165
P.O. Box LG 1279, Accra, Ghana

### 3.2.3 Time Zone

Greenwich Mean Time (GMT) throughout the year: GMT (UTC +0)

### 3.2.4 Telephone Numbers

0208110248
0207360545

### 3.2.5 Electronic Mail Address

csirt@garnet.edu.gh — this is a mail alias that relays mail to the human(s) on duty for GARNET CSIRT, feeding into GARNET's internal incident-tracking system so every report is logged and followed up.

### 3.2.6 Public Key and Encryption

PGP fingerprint: 684C 7B7D A77E 4F1B 68AE D3EC E84B 541C 6184 CC6F

The key is RSA 4096, expires 3 August 2028, and is published on the keys.openpgp.org keyserver and on csirt.garnet.edu.gh.

### 3.2.7 Team Members

Mr. Emmanuel Togo, Chief Technology Officer, is the GARNET CSIRT Coordinator. Mr. Samuel Kelly Brew and Mr. Emmanuel Vincent Mensah are GARNET CSIRT team members.

### 3.2.8 Operating Hours

Regular business hours (09:00–17:00 Monday to Friday, except public holidays).

### 3.2.9 Points of Customer Contact

The preferred method for contacting GARNET CSIRT is via email at csirt@garnet.edu.gh; mail sent to this address reaches the personnel on duty or is forwarded to the appropriate backup person. If you require urgent assistance, include "urgent" in the subject line. If email is not possible, GARNET CSIRT can be reached by telephone during regular office hours; telephone messages are checked less often than email.

## 3.3. Charter

This charter specifies the mandate of GARNET CSIRT and the authority under which it operates. It outlines the Mission Statement, Constituency, Sponsorship/Affiliation, and Authority of the CSIRT.

### *3.3.1. Mission Statement*

GARNET CSIRT's mission is to safeguard the cyber-ecosystem of Ghana's research and education community by building and maintaining the capability to detect, coordinate, and respond to computer and information security incidents across GARNET's member institutions, through proactive threat intelligence sharing, incident coordination, and capacity building for member institutions.

### *3.3.2. Constituency*

The constituency of GARNET CSIRT comprises all GARNET member institutions across Ghana's research and education community, represented through their designated IT and security staff.

### *3.3.3. Sponsoring Organization / Affiliation*

The GARNET Board is the sponsoring body of GARNET CSIRT. GARNET CSIRT is affiliated with WACREN and Ghana's Cybersecurity Authority (CSA).

### *3.3.4. Authority*

GARNET CSIRT operates as the coordinating CSIRT for GARNET members. It is responsible for coordinating, notifying, and supporting incident response across member institutions, and for facilitating escalation to regional and national bodies (WACREN, CSA) where necessary. GARNET CSIRT does not exercise operational authority over any member institution's internal security function; each member institution retains full responsibility for its own incident response.

## 3.4. Policies

### *3.4.1. Types of Incidents and Level of Support*

GARNET CSIRT will address all types of computer security incidents shared with it, and which occur or threaten to occur within its constituency.

GARNET CSIRT will do everything technologically possible to investigate, advise, coordinate, and monitor incidents, and to advise impacted institutions.

All incidents are treated as normal priority unless stated otherwise. GARNET CSIRT may, based on the circumstances, raise or lower the priority of an incident.

The level of support provided will vary depending on the type and severity of the incident, its potential or assessed impact, the institution affected, the size of the community affected, the urgency of the situation, and GARNET CSIRT's resources at the time.

### *3.4.2. Co-operation, Interaction and Disclosure of Information*

GARNET's internal technical team will cooperate internally in ensuring proper issue investigation and resolution. GARNET CSIRT will interact with member-institution CSIRTs and security teams, WACREN, CSA, vendors, and law-enforcement agencies to resolve issues beyond the capability of a single institution.

Collaboration between CSIRTs may lead to disclosure of information, for example reporting incidents within one institution's constituency to other teams outside it. GARNET CSIRT will be sensitive to local laws and regulations, which may vary across jurisdictions.

### *3.4.3. Communication and Authentication*

Telephones are considered sufficiently secure for use, even unencrypted. Unencrypted email is not considered particularly secure but is sufficient for low-sensitivity data.

Where it is necessary to establish trust, for example before relying on information given to GARNET CSIRT, or before disclosing confidential information, the identity of the other party will be ascertained to a reasonable degree of trust, using methods such as referrals from known trusted contacts within the GARNET membership, telephone call-back, or email mail-back to confirm the party is not an impostor.

## 3.5. Services

### *3.5.1. Incident Response*

GARNET CSIRT is available during regular business hours (09:00–17:00 Monday to Friday, except holidays) for services relating to computer incident response and handling.

The following are catered for as part of our services:

1. Preparation — implementing a set of controls based on the results of risk assessments.
2. Detection and Analysis — events are analyzed to determine whether they might constitute a security incident.
3. Containment, Eradication and Recovery — containment prevents an event or incident from spreading; eradication removes the threat; recovery restores affected systems to normal function.
4. Post-Incident Activity — to prevent or lessen the impact of future occurrences.

#### *3.5.1.1. Incident Triage*

All incidents reported go through the GARNET CSIRT triage process:

1. Collect more information on the reported case.
2. Collect targeted data for initial analysis.
3. Assess severity.
4. Assign a severity index (impact factor).

#### *3.5.1.2. Incident Coordination and Management*

This activity governs how a confirmed incident is run. GARNET CSIRT appoints an incident manager to coordinate the response, assembles the response team from GARNET CSIRT personnel and, where necessary, the affected institution's own staff and relevant third parties, and defines the roles and lines of communication for the duration of the incident. Updates to key stakeholders are maintained on a need-to-know basis throughout.

#### *3.5.1.3. Incident Resolution*

This activity concerns the outcome of the response. Working from the coordination structure above, GARNET CSIRT and the affected institution carry out the agreed remediation, confirm that affected systems and services are restored to normal operation, and close the incident once the immediate threat has been contained and recovery verified.

### *3.5.2. Proactive Activities*

GARNET CSIRT coordinates and maintains the following services for its membership:

- Proactive threat and credential-compromise notifications: GARNET CSIRT monitors external threat intelligence feeds and notifies affected member institutions of compromised credentials or other exposures relevant to their networks.
- Security advisories and mailing lists: to inform member institution security contacts of new information relevant to their computing environments.

- Training and awareness: GARNET CSIRT runs periodic workshops (such as the Network Monitoring & Management workshop series) covering network security and monitoring topics for member institution IT staff.
- Log archiving: GARNET operates internal logging pipelines for DNS resolution and RADIUS authentication (eduroam) traffic across the membership.

### 3.6. Incident Reporting

Incidents are reported to GARNET CSIRT via email at csirt@garnet.edu.gh. This is the single official reporting channel; all reports are logged in GARNET's incident-tracking system to ensure every case is tracked to resolution. GARNET CSIRT does not currently accept incident reports via WhatsApp or other messaging channels, in order to keep all reporting auditable within one system.

### 3.7. Disclaimers

GARNET CSIRT will only respond to incidents that are reported through its official communication channel. Hearsay and rumours will not be considered as incidents.

## 4. Standards and Basis

This charter follows the structure recommended by RFC 2350 (Expectations for Computer Security Incident Response) and draws on the CSIRT establishment and operational guidance published by FIRST (the Forum of Incident Response and Security Teams). Aligning to these recognised standards is intended to make GARNET CSIRT's scope, services, and contact expectations clear and interoperable with the wider incident-response community.

## 5. References

www.csirt.org/sample_policies

www.exabeam.com/incident-response/csirt/

www.ietf.org/rfc/rfc2350.txt

https://datatracker.ietf.org/doc/html/rfc2350

## 6. Security Considerations

This document describes the operation of GARNET CSIRT and its interactions with its constituency and other organisations. It is not directly concerned with the security of protocols, applications, or network systems themselves, nor with the technical details of responses to security incidents, only with an appropriate description of the services GARNET CSIRT provides. Nonetheless, it is vital that GARNET CSIRT itself operates securely: establishing secure communication channels with other teams and constituents, securing its own systems and infrastructure, and maintaining the confidentiality of the identity of victims and reporters of security incidents.

## 7. Author's Addresses

Mr. Emmanuel Togo
Chief Technology Officer
Ghanaian Academic and Research Network (GARNET)