Service Description: Incident Handling

1 Definition

Incident handling involves receiving, triaging, and responding to requests and reports, and analysing incidents and events. Particular response activities can 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

2 Objectives

- To provide technical support to RENU in response to computer security incidents.
- To ensure the security of RENU's network infrastructure.
- To act as a liaison of RENU to other CSIRT teams and other third parties during incident response.

3 Inputs

To facilitate the handling of an incident, the incident needs to be reported first, as shown in Phase 1 in Figure 1 below. The RENU-CERT requires specific information about an incident as it is reported by its constituents or other parties. This information is collected via the reporting forms available on the RENU-CERT website <link>. See Report form fields for more details on what information is required in an incident report to the RENU-CERT. Submission of these reports can be done through the stated communication channels; i.e. via email or telephone. In the case of telephone, the RENU-CERT member will fill in the report as they talk with the constituent about the incident being reported.

4 Function Description

The incident handling service usually includes other activities that support the delivery of the service, consisting of the triage and handling functions. These functions and their relationships are illustrated in Figure 1 below and are covered in more detail thereafter.

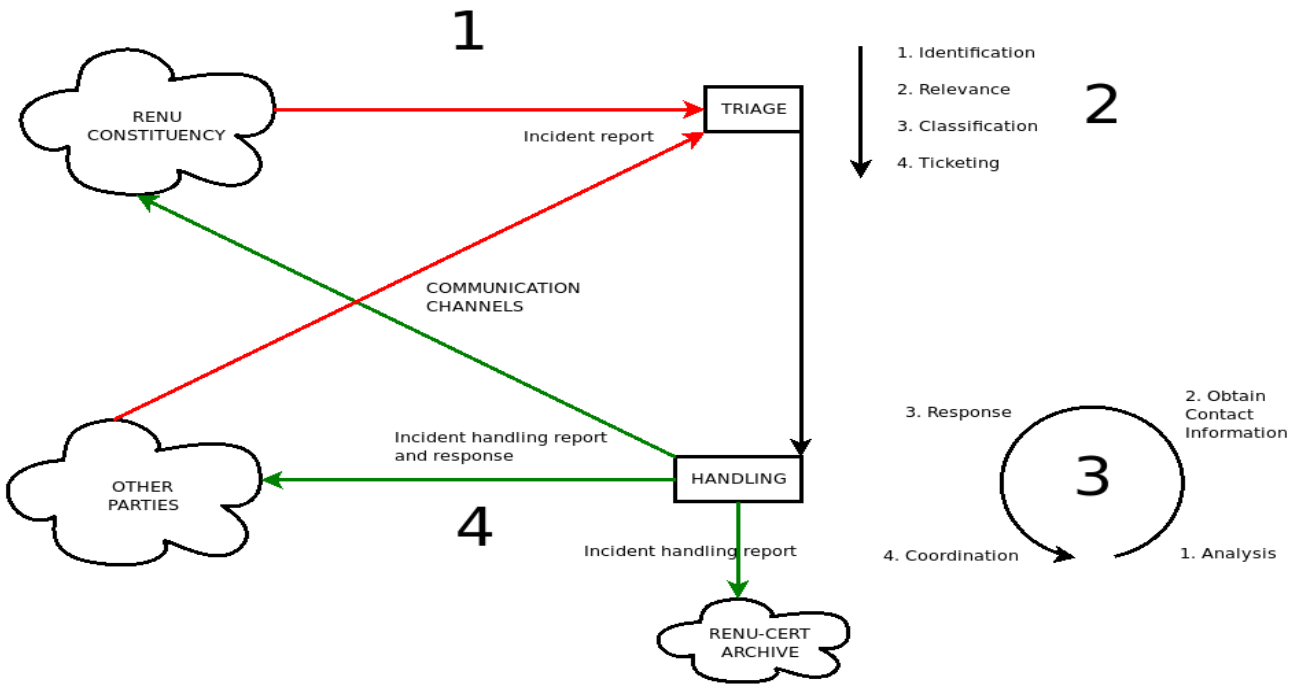

Figure 1: Incident Handling service flowchart

4.1 Triage

The goal of this function is to ensure that all incident reports destined for the incident handling service are channelled through a **single** focal point regardless of the method by which it arrives (e.g. by email or telephone) for appropriate redistribution and handling within the service. It is where an incident can be initially categorized, identified as a new event to track or as part of some existing incident already being tracked. The appropriate tracking number is assigned to it (either a new tracking number or the number for an activity already being tracked and to which it belongs). Note that a new incident can also be identified during the handling function (see Handling) as a result of incorrectly triaged information, information provided to the team under an incorrect tracking number, or new information being discovered as a result of more in-depth technical analysis. The activities in this function include the identification, relevance, classification and ticketing of incoming incident reports, as shown in Phase 2 in Figure 1 above and as detailed below.

1. **Identification** – An incoming report always has to be identified by its **source** and it has to be determined whether the source is **authentic** before any action can be taken.
2. **Relevance** – The incident-handling request is checked to see whether it originates from the constituency, or if the reported incident involves IT systems from the constituency.
3. **Classification** – The category and level of severity of the incident is determined at this step. See Quality Assurance below.
4. **Ticketing** – The incident is identified as a new event to track or as part of some existing incident already being tracked. The appropriate tracking number is assigned to it (either a new tracking number or the number for an activity already being tracked and to which it belongs).

4.2 Handling

The handling function provides support and guidance related to suspected or confirmed computer security incidents, threats, and attacks. The goal of this function is to provide response and support for reports received from the constituency (and possibly others). This process is done in the life-cycle shown on Phase 3 in Figure 1 above. Note that the handling process might under go multiple iterations before it is resolved. The activities in this function include:

1. **Incident Analysis** – All details of the reported incident are analysed such as log files, affected sites. See Analysis.
2. **Obtain contact information** – To be able to further report information related to the incident to all involved parties.
3. **Incident Response** - Help victims to quickly recover from the results of the incident and collect more information about the attack. See Response.
4. **Incident Response Coordination** - Inform other involved parties like the entity responsible for the IT system used for an attack, or other victims. See Coordination.

5 Outputs

At the closure of the resolved incident (Phase 4 shown in Figure 1 above), the RENU-CERT will mark the incident as closed, informing all concerned parties about its closure. Along with the closure, the RENU-CERT will generate an **Incident Handling Report(s)** showing all the steps taken and other evidence gathered during the incident handling process. See Incident Handling Report format for details. The report(s) will be disseminated to the various parties involved, with varying levels of detail, with the one to the reporter being the **most** detailed. Copies of these reports will be archived by the RENU-CERT for use in resolving similar future incidents faster, drawing lessons learnt by the team internally and for generating other documents such as advisories and announcements to be consumed or acted upon by the constituency.

6 Availability

This service is available to the entire RENU constituency; i.e. the RENU member institutions **and** the team at the RENU Secretariat site.

The service is available **24/7** and the team will receive reports via the stated communication channels; i.e. email and telephone. However, **On-site** incident response will be available **only** during **working** hours. During **non-working** hours, reports will be received **only** via telephone and **only** incidents of Criticality Level **1** will be handled.

During the execution of this service, the reporting constituent should expect feedback via an email or telephone notification on:

- the acknowledgement of receipt of their report(s),
- the progress of the handling of the incident,
- any other required coordination response support.

7 Quality Assurance

The quality of this service depends on the **Criticality Level** and **Reporting Time** of incoming incident reports.

- The **Criticality Level** of a reported incident is a measure of how much that incident negatively affects the critical systems or information of, and its potential to be revenue- or customer-impacting to the reporting constituent or other party. This metric cuts across all incident categories supported.
- The **Reporting Time** of an incident is the time that incident was reported by the reporting constituent or other party.

The parameters to measure the quality at which the RENU-CERT renders this service are as follows:

- **Maximum incident report acknowledgement (ACK) time**, which is defined as the maximum amount of time the RENU-CERT should take to send a notification to the sender acknowledging that they have received a report on a given incident. This applies to reports submitted by email.
- **Maximum incident resolution time**, which is defined as the maximum amount of time the RENU-CERT should take to resolve a reported incident.

The service quality assurance matrices are as shown below.

Criticality Level	**Criticality Level description**	**Maximum incident resolution time**
1	Incident affecting critical systems or information with potential to be revenue- or customer-impacting.	3 working days
2	Incident affecting **non**-critical systems or information, **not** revenue- or customer-impacting. Other investigations that **are time-sensitive** should typically be classified at this level.	7 working days
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 research and/or detailed forensic work are also classified at this level.	14 working days

NB:

- If any incident is not resolved within the maximum resolution time associated with its Criticality Level, then a notification will be immediately sent out to all concerned parties by the RENU-CERT explaining why the incident has not yet been resolved. Thereafter, the RENU-CERT shall continue to work to resolve the incident in a manner that corresponds to its Criticality Level. For example, if a Criticality Level 1 incident is not resolved in 3 working days, the notification is sent and work is resumed to resolve it within the following 3 working days since it's still a Criticality Level 1 incident.
- The handling of incidents will be scheduled according to their Criticality Levels, with the more critical ones handled first. Put another way, the incidents will be handled in an **Earliest Deadline First (EDF)** scheduling approach.

Reporting Time	**Maximum incident report ACK time**	**Criticality Level of incidents handled**
During working hours	1 hour	1, 2, 3
During Non-working hours	2 hours	1

7.1 Incident Categories

This service handles incidents that fall directly into the categories as shown below.

Category	**Description**
Denial of Service	DoS or DDoS attacks
Compromised Asset	Compromised host (root account, Trojan, rootkit), network device, application, user account. This **includes** malware-infected hosts where an attacker is actively controlling the host.
External Hacking	Reconnaissance or Suspicious Activity originating from **outside** the RENU network (partner network, Internet), excluding malware.
Internal Hacking	Reconnaissance or Suspicious activity originating from **inside** the RENU network, excluding malware.
Malware	A virus or worm typically affecting multiple devices in RENU. This **does not include** compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	Spoofed email, SPAM, and other email security-related events.
Policy Violation	Inappropriate use of corporate asset such as computer, network, or application. Non-compliance to RENU Information Security Policy.

8 Interface with other services

During the handling phase of this service, the steps necessary to resolve an incident might involve **on-site incident response** and therefore, will call upon this service directly at the point of providing

technical support. To add to this, **generating announcements and alerts** to the RENU constituency might be necessary during the handling of an on-going incident in order to minimise its possible spread.

The incident handling report generated at the end to the handling process is archived for use in analysis of future related incidents and serves as a reference point for lessons learnt internally for the RENU-CERT. The archive of reports also serves as an **input** information source for the **Security-related information dissemination service,** in that it provides information for generating advisories, announcements and alerts. It also provides input into the assessment of the RENU constituency's installation base to better customise the information disseminated by the RENU-CERT to its constituents.

9 Information disclosure and interaction

9.1 Information from the constituent

This information will be availed to the RENU-CERT via a report form, available at the RENU-CERT website <link>, 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. This information to disclose might include:

- Incident tracking number
- Incident category
- 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.

9.2 Information from the RENU-CERT

After the reported incident has been resolved, the RENU-CERT shall generate and send an incident report to the reporter containing full details of the handling procedures, while a less detailed report will be generated and sent to other involved parties. This will mark the closure of the said incident by the RENU-CERT and its closure will be communicated to all affected or involved parties.

APPENDIX

1 Incident Handling Activities

1.1 Analysis

There are many levels of incident analysis and many sub-services. Essentially, incident analysis is an examination of all available information and supporting evidence or artifacts related to an incident or event. The purpose of the analysis is to identify the scope of the incident, the extent of damage caused by the incident, the nature of the incident, and available response strategies or workarounds. The RENU-CERT may use the results of vulnerability and artifact analysis (described below) to understand and provide the most complete and up-to-date analysis of what has happened on a specific system. The RENU-CERT correlates activity across incidents to determine any interrelations, trends, patterns, or intruder signatures. Two sub-services that may be done as part of incident analysis are:

Forensic evidence collection

The collection, preservation, documentation, and analysis of evidence from a compromised computer system to determine changes to the system and to assist in the reconstruction of events leading to the compromise. This gathering of information and evidence must be done in a way that documents a **provable** chain of custody that is **admissible** in a court of law under the rules of evidence. Tasks involved in forensic evidence collection include (but are not limited to) making a bit-image copy of the affected system's hard drive; checking for changes to the system such as new programs, files, services, and users; looking at running processes and open ports; and checking for Trojan horse programs and toolkits.

Tracking or tracing

The tracing of the origins of an intruder or identifying systems to which the intruder had access. This activity might involve tracking or tracing how the intruder entered the affected systems and related networks, which systems were used to gain access, where the attack originated, and what other systems and networks were used as part of the attack.

1.2 Response

Incident response support

The RENU-CERT assists and guides the victim(s) of the attack in recovering from an incident via telephone, email or documentation. This can involve technical assistance in the interpretation of data collected, providing contact information, or relaying guidance on mitigation and recovery strategies. The RENU-CERT instead provides guidance **remotely** so site personnel can perform the recovery themselves.

Incident response on site

The RENU-CERT provides direct, **on-site** assistance to help constituents recover from an incident. The RENU-CERT itself travels to the constituent's site and performs the response **physically**, instead of only providing incident response support by telephone or email. This service involves all actions taken on a local level that are necessary to mitigate the incident if one is suspected or occurs. This service is only activated when the Incident response support service (see above) fails to mitigate the incident.

Vulnerability response

This service involves determining the appropriate response to mitigate or repair a vulnerability. It also involves notifying others of the mitigation strategy, possibly by creating and distributing advisories or alerts. This service can include performing the response by installing patches, fixes, or workarounds.

Artifact response

An artifact is any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures. Artifacts can include but are not limited to computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits. This service therefore involves determining the appropriate actions to detect and remove artifacts from a system, as well as actions to prevent artifacts from being installed. This may involve creating signatures that can be added to antivirus software or IDS.

1.3 Coordination

Incident response coordination

The CSIRT coordinates the response effort among parties involved in the incident. This usually includes the victim of the attack, other sites involved in the attack, and any sites requiring assistance in the analysis of the attack. It may also include the parties that provide IT support to the victim, such as Internet service providers, other CSIRTs, and system and network administrators at the site. The coordination work may involve collecting contact information, notifying sites of their potential involvement (as victim or source of an attack), collecting statistics about the number of sites involved, and facilitating information exchange and analysis. This service does not involve direct, on-site incident response.

Vulnerability response coordination

The RENU-CERT notifies the various parts of the RENU constituency about the vulnerability and shares information about how to fix or mitigate the vulnerability. This service may involve communicating with vendors, other CSIRTs, technical experts, RENU constituents, and the individuals or groups who initially discovered or reported the vulnerability. This service can also include maintaining a public or private archive or knowledge base of vulnerability information and corresponding response strategies.

Artifact response coordination

This service involves sharing and synthesizing analysis results and response strategies pertaining to an artifact with the RENU constituency, other CSIRTs, vendors, and other security experts. Activities can also include maintaining a public or constituent archive of known artifacts and their impact and corresponding response strategies.

2 Report form fields

* - required information

2.1 Information fields from RENU constituency

- Name and Organisation
  - Name*
  - Constituency site (Member Institution)*
  - Email Address*
  - Telephone Number*
  - Other
- Affected host(s)
  - Number of hosts
  - Hostname and IP address*
  - Function of the host*
  - Hardware
  - Operating System
  - Affected software
  - Affected files
  - Protocol – UDP/TCP
  - Port number
- Incident Report Details
  - Start time
  - Time of discovery*
  - Method of discovery*
  - Detailed description* - attach any supporting documents (log files, screenshots, error messages, network traces, etc)

2.2 Information fields from other parties

- Name and Organisation
  - Name*
  - Name of Organisation*
  - Sector type
  - Country*
  - City
  - Email Address*
  - Telephone Number*
  - Other
- Affected Host(s)
  - Number of hosts
  - Hostname and IP address*
  - Function of the host*
  - Time-Zone
  - Hardware
  - Operating System
  - Affected software
  - Affected files
  - Protocol – UDP/TCP
  - Port number
- Incident
  - Incident category* – include table
  - Criticality level* – include table
  - Start time
  - Time of discovery*
  - Method of discovery*
  - Detailed description* - attach relevant documents (log files, screenshots, network traces, etc)

3 Incident Handling Report format

- Tracking Number (RENU-CERT:INC:#)
- Report Summary
  - receipt timestamp
- Triage
  - Start / receipt ACK timestamp
  - Incident Category
  - Criticality Level
- Handling
  - Start timestamp
  - Analysis and Interpretation
  - Response and Coordination
  - Resolution timestamp
- Conclusions and Lessons learnt
- References
- Appendix
  - Log files
  - Screenshots
  - Anything else useful