University of Ibadan

Information Technology and Media Services [ITeMS]

A Proposal for a

Computer Security Incident Response Team (CSIRT)

with
Draft Operational Standards, Guide and Policy

Dr O. Osunade *FNCS*
Director, Information Technology and Media Services [ITeMS]

April, 2017

E-mail: o.osunade (at) ui.edu.ng.

Table of Contents

1.0 INTRODUCTION

What the University of Ibadan Internet community will face in terms of Internet security in the next few years can be summarized in the following statements:

- the number of companies and users of the Internet is increasing
- the vendor product development and testing cycle is decreasing
- the complexity of protocols and applications run on clients and servers attached to the Internet is increasing
- the complexity of the Internet as a network is increasing
- the information infrastructure has many fundamental security design problems that cannot be quickly addressed
- the expertise of intruders is increasing
- the sophistication of attacks, intruder tools, and toolkits is increasing
- the number of computer security intrusions is increasing
- the effectiveness of intruders is increasing (knowledge is being passed to less knowledgeable intruders thus making them effective)
- the number of people with security knowledge and expertise is increasing, but at a
- significantly smaller rate than the increase in the number of Internet users
- the number of security tools available is increasing, but not necessarily as fast as the complexity of software, systems and networks
- the number of incident response teams is increasing, but the ratio of incident response personnel to Internet users is decreasing

Aggressive, coordinated response will continue to be necessary, but UI must also move quickly to put other solutions in place to achieve the following:

- higher quality information technology products with security mechanisms that are better matched to the knowledge, skills, and abilities of today's system managers, administrators, and users
- expanded research programs that lead to fundamental advances in computer security
- large number of technical specialists who have the skills needed to secure large, complex systems
- increased and ongoing awareness and understanding of cyber-security issues, vulnerabilities, and threats by all stakeholders in cyber space

Keeping University of Ibadan information assets secure requires a multi-layered approach. There is no one action or solution that is a panacea. Creating a Computer Security Incident Response Team (CSIRT) is one layer, along with implementing secure configurations, security awareness training, and external and internal defenses.

Much like a fire department, a CSIRT can perform both reactive and proactive services. A fire department responds to and extinguishes fires. They also proactively provide fire-prevention training, promote the installation of smoke alarms and purchasing of fire escape ladders, and instruct families in the best manner to safely exit a burning building. CSIRT help to protect computer communication channels, restore damaged information services and detect the presence of intruders on a network.

Many organizations start thinking about how to handle a computer security incident after an intrusion has occurred. University of Ibadan has had its fair share of incidents such as e-mail server crash, loss of Internet connectivity and spam emails.

ITeMS has been handling all security incidents, thus the establishment of a CSIRT will formalize the operations, processes and policies.

A variety of acronyms have appeared and are used to represent different response teams. Here are a few examples:

CERT Computer Emergency Response Team
CSIRT Computer Security Incident Response Team
CSIRC Computer Security Incident Response Capability

CIRT Computer Incident Response Team
CIRC Computer Incident Response Capability
IRT Incident Response Team
SERT Security Emergency Response Team
SIRT Security Incident Response Team

For the operations of University of Ibadan and ITeMS, the acronym CSIRT will be used throughout this document and adopted for its implementation.

1.1 CSIRT Benefits

There are several qualitative and quantitative benefits that can be achieved, for both ITeMS and the users by implementing an effective and efficient Incident Management process. The Incident Management process life cycle requires:

- Capturing accurate data across ITeMS to analyze the level of resources applied to the Incident Management process
- Informing units of the services ITeMS provides and the level of support and maintenance required for ongoing service levels
- Minimize impacts to university functions by resolving incidents in a timely manner
- Providing the best quality service to all users

1.1.1 Benefits to ITeMS

Incident Management is highly visible to the university and it is easier to demonstrate its value than most areas in Service Operation. A successful Incident Management process can be used to highlight other areas that need attention:

- Improved ability to identify potential improvements to IT services
- Better prioritization of efforts
- Better use of resources, reduction in unplanned labor and associated costs
- More control over IT services
- Better alignment between departments
- More empowered IT staff
- Better control over vendors through Incident Management metrics

1.1.2 Benefits to Users

- Higher service availability due to reduced service downtime
- Reduction in unplanned labor and associated costs
- IT activity aligned to real-time business priorities
- Identification of potential improvements to services
- Identification of additional service or training requirements for the business or IT

1.2 Operational Standards Document Overview

This document defines the establishment of a computer security incident response team at University of Ibadan, Nigeria.

The Computer Security Incident Response Team (CSIRT) will follow the operational standards in this document. The standards provide a formalized approach to computer/network incident identification, investigation, and reporting. The standards will be periodically updated to reflect the changing technology environment and campus needs. Request for changes to the CSIRT standards should be forwarded to the university designated Security Manager (csirt@ui.edu.ng).

If there are conditions under which the applicability of the standards is unclear, it is the responsibility of the user to seek interpretive guidance from the CSIRT Chair or Security Manager.

2.0 ESTABLISHMENT OF CSIRT

2.1 CSIRT Purpose

CSIRT is responsible for establishing, overseeing, and carrying out plans of action for any incident that potentially threatens the confidentiality, integrity, or availability of University electronic information assets and/or computing resources.

The CSIRT team will work closely with the Director Information Technology and Media Services [ITeMS] Office on the development of operational procedures for and documentation of incidents.

CSIRT Team members will develop policies and procedures for the prevention, identification, analysis, containment, and eradication of security threats. They will restore/recover the information or computing resource to an operational state as quickly as possible while preserving forensic data. Team members also serve as liaisons to the University department(s) where the incident occurs throughout the response process.

2.2 CSIRT Overview

The CSIRT is a group comprised of technology and functional specialists from the University Library, Directorate of Information Technology and Media Services [ITeMS], Registry (Establishments, Legal and Records), Bursary and University Health Services involved/charged with the prevention, identification, analysis, containment, and eradication of computer/network security incidents.

Security incidents are events that could adversely affect University of Ibadan computer or network resources and/or cause loss of or damage to electronic information resources.

2.3 CSIRT Goals

The overall goal of the CSIRT is to protect and preserve electronic information and computer/data network assets to ensure the availability, integrity and, as required, confidentiality, of university electronic information and network assets.

2.4 CSIRT Objectives

There are five primary objectives of CSIRT:

1. Control and manage the incident
2. Timely investigation and assessment of the severity of the incident
3. Timely recovery or bypass of the incident to normal operating conditions
4. Timely notification of serious incidents to senior campus administrators

5. The prevention of similar incidents in the future

3.0 CSIRT ORGANIZATION

University response to computer/network security incidents is handled within a framework of the University of Ibadan Information Security Advisory Group (UISAG) and CSIRT. The chair of CSIRT reports to the Director, Information Technology and Media Services [ITeMS].

Figure 3.0.1 Shows the organizational chart for the CSIRT at University of Ibadan. Brief explanations of each position is given.

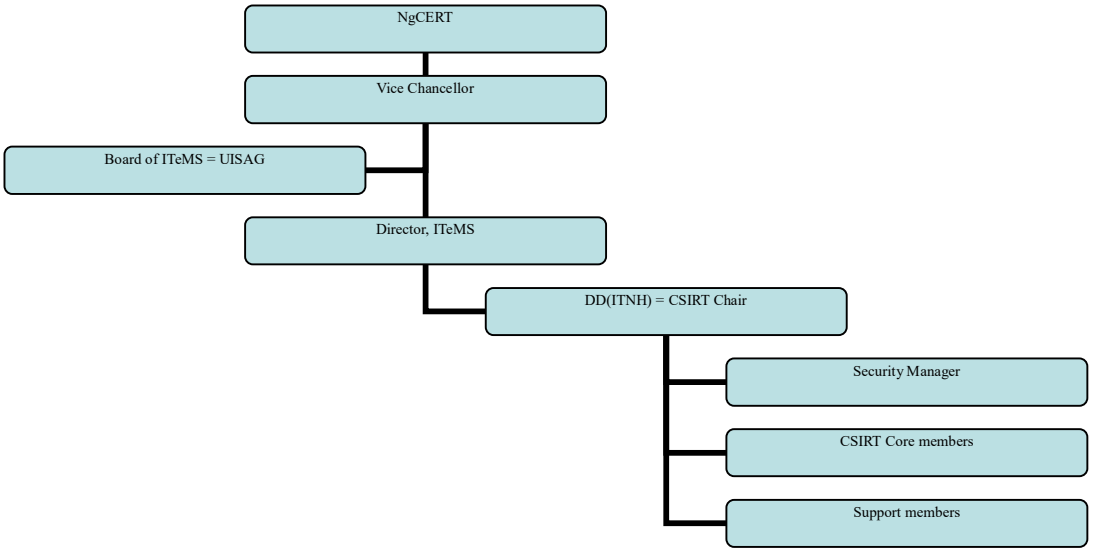


Figure 3.0.1 UI-CSIRT Organizational chart

3.1 NgCERT
The Federal Republic of Nigeria has a Computer Emergency Response Team (NgCERT) located in the Office of the National Security Adviser (ONSA). Further details are provided in the Appendix.

3.2 Vice Chancellor (VC)
The Vice Chancellor represents the authority of the University. The VC should be informed of all external communications with the NgCERT. The VC can report an incident or close an incident.

3.3 University Information Security Advisory Group (UISAG)
The University of Ibadan ISAG is charged with guiding the development and maintenance of University plans and policies designed to preserve the confidentiality, integrity, and availability of University electronic information assets and/or computing resources. The University of Ibadan ISAG provides policy guidance and support for CSIRT. The Board of Information Technology and Media Services [ITeMS] will serve this purpose.

3.4 Director, Information Technology and Media Services [ITeMS]
The Director [ITeMS] is responsible for the daily operations and leadership of Information Technology and Media Services. The role will support the CSIRT, provide resources and serve as bridge to the UISAG and NgCERT.

3.5 CSIRT
CSIRT is the operational team of specialists responsible for conducting an incident investigation and recommending measures to correct or bypass a problem or condition relating to the incident. The nature of the incident will determine the actual role CSIRT will have in respect to implementing a corrective or

preventive action.

The actual team consists of a core team who are assisted by support team members (subject matter experts), depending on the nature of a particular incident under investigation.

3.5.1 CSIRT – Chair
The Information Technology, Network and Hardware (ITNH) Deputy Director acts as CSIRT Chair and Security Manager. The chair approves initiation of a CSIRT investigation and CSIRT activities performed in support of the investigation. Responsibilities include:

- Convene CSIRT
- Conduct CSIRT meetings
- Coordinate CSIRT investigation
- Ensure incidents are classified according to severity class
- Determine investigation objectives
- Define/obtain resource requirements
- Communicate with external agencies through the Director [ITeMS]
- Coordinate CSIRT training and exercises
- Prepare post-investigation "Lessons Learned" analysis
- Request support team resources
- Prepare CSIRT management reports
- Consult with Director, Information Technology and Media Services [ITeMS]on incidents classified with a medium or high severity rating
- Communicate with senior department managers regarding incident investigation status
- Arrange for responsibility coverage during temporary absences

3.5.2 CSIRT - Core Team Members
CSIRT members include information technology representatives from each unit within the University. These core team members are specialists with operating system, telecommunication, network, and/or database knowledge and skills.

3.5.3 CSIRT - Core Team Responsibilities
The primary responsibilities of the CSIRT are investigation and reporting. In order to carry out these responsibilities, the following support activities will be performed by the CSIRT:

- Maintain availability for 40 hours a week (i.e. Monday – Friday 08:00am-04:00pm) communication access and incident response
- Develop and maintain incident classification scheme
- Monitor University of Ibadan campus reporting mechanisms for reports of incidents
- Notify and consult with Security Manager
- Assess scope of incident damage
- Classify incidents by severity
- Determine if incident can be investigated
- Control and contain incident
- Collect, document and preserve incident evidence
- Maintain chain of custody of all incident evidence
- Interview individuals involved in incident
- Conduct investigation to identify incident root cause or source, extent of damage, and recommended counter action
- Coordinate release of information with public relations staff
- Consult with law enforcement agencies, as authorized
- Follow all policies, laws, and regulations relating to privacy
- Prepare reports describing incident investigations
- Prepare recommendations to prevent future similar incidents

- Prepare recommendations to resolve incident and/or reduce impact of incident
- Prepare recommendations to bypass or correct conditions leading to incident
- Monitor recovery
- Identify CSIRT operational improvements
- Assist recovery from incident, where applicable

3.5.4 CSIRT - Support Team Members

Support members are not permanent CSIRT members. The support team members have expertise in particular subject matter that could be relevant to a CSIRT investigation. The CSIRT chair will determine when such expertise is required during an investigation. The support member will be added to the incident team at that time. Any security incident investigation which includes a departmental computing system not under complete administrative control of ITeMS will be conducted by a minimum of two CSIRT members in addition to a representative of the department responsible for the computing system under review.

Support Team members will typically be drawn from the following areas:

- Departmental Technical Support Coordinator: When the target of the security incident is a departmental computing/network system, not administered by ITeMS staff, the CSIRT will include a Technical Support Coordinator from the impacted department.
- Platform Specialists (e.g., Operating Systems, Applications, Hardware)
- Telecommunication Specialists (e.g., Network Infrastructure, Wireless, Telephones)
- Public Relation Specialists
- Human Resource Specialists
- Internal Auditors
- Public Safety/Law Enforcement Investigators

3.5.5 Support Team Responsibilities

The primary responsibilities of the CSIRT Support Team members are to assist CSIRT Core Team investigation and reporting. The Support Team members provide professional and technical expertise to the CSIRT core team in special subject knowledge areas.

Typical responsibilities of Support Team members include:

- Assess scope of incident damage
- Assist classification of incidents by severity
- Assist determination whether incident can be investigated
- Assist control and containment of incident
- Collect, document and preserve incident evidence
- Maintain chain of custody of all incident evidence
- Interview individuals involved in incident
- Assist investigation to identify incident root cause or source, extent of damage, and recommended counter action
- Provide public communications guidance
- Provide guidance regarding law enforcement role
- Follow all policies, laws, and regulations relating to privacy
- Assist preparation of reports describing incident investigations
- Assist preparation of recommendations to prevent future similar incidents
- Assist preparation of recommendations to resolve incident and/or reduce impact of incident
- Assist preparation of recommendations to bypass or correct conditions leading to incident
- Assist in monitoring recovery
- Assist recovery from incident, where applicable
- Identify CSIRT operational improvements

3.5.6 CSIRT Relationship to Other University Departments

The following departments/units may also be involved with response to an incident:

- Works and Maintenance Unit
- Equipment Maintenance Centre
- Security Unit
- Audit Unit
- Student Affairs Unit
- Directorate of Public Communications
- Establishments Division (Academic and Non-teaching Staff)
- External vendor e.g. Onet, IPNX, SocketWorks

4.0 CSIRT OPERATIONAL RESOURCES

In order to conduct incident response investigations, CSIRT needs to acquire and maintain selected investigation tools. In addition, CSIRT needs to have a physically secured location to store investigation tools, conduct investigation analysis, and store material collected and/or prepared during the incident investigation. The following operational resources may be used by CSIRT:

- Hardware
  - o Portable data storage devices
  - o Workstations (Multi-OS or VMWare)
  - o Forensic toolkit
  - o Dedicated, Permanent High-Volume Storage Area

- Software
  - o Forensic analysis
  - o Forensic imaging
  - o Password recovery
  - o Encryption Software
  - o Cryptographic Hash Utilities
  - o Ticket / Incident Tracking System

- Miscellaneous Supplies
  - o Photographic Imaging Equipment
  - o Portable evidence storage containers
  - o Spare backup media
  - o Locking file cabinets
  - o Secured physical room with restricted entry

5.0 CSIRT Training

CSIRT team members are required to obtain training and periodic updates in the following knowledge and skill areas:

- State and Federal Laws
- University of Ibadan policies
- Investigative processes
- Information Security
- Ethical hacking
- Evidence handling and protection
- Technical CSIRT hardware and software tools
- Testimony skills

6.0 CSIRT EXERCISES

UI CSIRT will conduct an annual exercise that simulates a computer security incident. The purpose of the

exercise will be to maintain the skills and knowledge of CSIRT members. The exercises will involve all CSIRT core team members. Support team members may be selected to participate as required by the nature of the exercise. At the termination of the drill, the CSIRT Chair will prepare a brief report to the UISAG through Director [ITeMS] evaluating the exercise. Any skill and/or knowledge area that needs to be improved as well as procedural enhancements should be identified in the report.

7.0 INCIDENT DEFINITION

For the purposes of this document and ITeMS, an incident is defined as an event that has actual or potential adverse effects on computer or network resources resulting in misuse or abuse, compromise of information, or loss or damage of property or information. Any such events that originate from, are directed towards, or transit University controlled computer or network resources will fall under the purview of CSIRT.

This definition is purposely made inclusive, however it is foreseen that many events classified with a "limited" severity rating may be handled by semi-automated means and not require any further escalation. Incident types include, but are not limited to: Compromised Machine, Denial of Service, Hoax, Malicious Code, Policy Violation, Probe, Unauthorized Access, Unauthorized Use.

8.0 REPORTING NEW INCIDENTS & USER NOTIFICATION

An incident can be reported through existing central reporting mechanisms at the Information Technology and Media Services office. A university community member or anyone affected by a security incident should report a suspected incident by e-mail (abuse@ui.edu.ng).

In addition, CSIRT will coordinate with all ITeMS departments to ensure that CSIRT is notified of any reported problem that may reflect a security incident. The individual reporting the incident will be asked to provide date, time, timezone, user contact information, brief description of the incident, and, if available, source and target network information.

Acknowledgement of a reported incident by CSIRT shall occur via an auto-generated response to email or web notifications. A telephone-reported incident will be acknowledged with a telephone call or email message from the CSIRT. All user reports will be analyzed, classified by severity rating, and an appropriate response will be generated.

The scope of CSIRT response will be determined by the incident severity rating, or as directed by the Security Manager. If the nature of the incident cannot be reported via non-confidential methods, the incident may be directly reported to the Security Manager, CSIRT Chair or Director, Information Technology and Media Services [ITeMS].

All communication between CSIRT members and externally will adhere to the Traffic Light Protocol (TLP) as it relates to privacy. The Traffic Light Protocol is given in the appendix.

8.1 Incident Priority

The priority of an incident is determined by:

1. **Impact**: Impact of the incident on the university. The number of users or importance of system affected. The hierarchical position of the client is included in this variable.

2. **Urgency**: How severely the user's work process is affected. This influences the timeframe that is allowed to resolve the incident.

The Impact/Urgency matrix, shown below, determines the priority of the incident.

		Impact		
		Low	**Medium**	**High**
Ur	**Low**	5	4	3
	Medium	4	3	**2**

	High	3	**2**	**1**

The assessment methodology for the impact and the severity is explained in more detail in the sections below.

8.1.1 Impact

Incidents will be placed into High, Medium and Low impact categories. The key factor in measuring impact is the **impact the incident has on the university**. Each incident will be reviewed on a case-by-case basis with appropriate impact assessment and approval based on the following criteria.

Impact	Description
High	Whole organisation affected; Site or multiple sites affected; Multiple groups of users affected; Critical business process interrupted; or System-wide outages to Student Portal, Internet access, website or Email
Medium	Group of clients, Vice Chancellor (VC), Principal Officers, or a member of the Vice Chancellors (VC's) Office staff affected; Non-critical university process interrupted.
Low	One client affected (other than VC's Office or Principal Officers)

8.1.2 Urgency

Incidents will be placed into High, Medium and Low urgency categories. The key factor in measuring urgency is how severely the **user's work process** is affected. This influences the timeframe that is allowed to resolve the incident. Each incident will be reviewed on a case-by-case basis with appropriate severity assessment and approval based on the following criteria.

Urgency	Description
High	Process stopped; user(s) cannot work
Medium	Process affected; user(s) cannot use certain functions
Low	Process not affected; change request, new/extra/optimised function

9.0 TIME TO RESOLVE INCIDENTS

The CSIRT should establish timelines for handling incidents. The table below shows suggested target time frames for University of Ibadan

Priority	Target	
	Response	Resolve
3 - Low	90% - 24 hours	90% - 7 days
2 - Medium	90% - 4 hours	90% - 7 hours
1 - High	95% - 60 minutes	90% - 3 hours

10.0 INCIDENT CLASSIFICATION ESCALATION/DE-ESCALATION

All new incidents will be assigned a severity rating by the CSIRT Chair in consultation with the CSIRT members. Such incident ratings may change over the course of an incident as more information about the incident becomes available and is reviewed by the CSIRT. The CSIRT Chair, in consultation with the CSIRT members, will determine if an incident rating should be escalated or deescalated. The same criteria used to initially rate a newly reported incident will be used to escalate or deescalate an incident severity rating.

10.1 Incident Severity Escalation

If an incident is escalated to a "medium" rating, the CSIRT Chair shall inform core team members and Director [ITeMS] via email about the incident and the reason for the escalation. This escalation shall be communicated to all CSIRT members.

If an incident is escalated from a "low" or "medium" severity rating to a "high" severity rating, the CSIRT Chair will review the incident with appropriate members of the CSIRT via telephone or an ad hoc meeting. The Security Manager will notify the Director, Information Technology and Media Services [ITeMS] through the CSIRT Chair in regards to any "high" severity rated incident and its possible campus impact.

10.2 Incident Severity De-escalation

The CSIRT Chair may determine an incident rating should be de-escalated to a "medium" or "low" category. If a "high" severity incident is downgraded to a "medium" or "low" severity rating, the CSIRT Chair must receive approval from the Director, Information Technology and Media Services [ITeMS] and the user. In such cases, the reason for the de-escalation shall be documented within the incident investigation.

If the incident was previously rated as "medium" and is downgraded to "low", the appropriate members of the CSIRT shall be informed about this action and the justification of the change.

11.0 INCIDENT INVESTIGATION/MANAGEMENT PROCESS

The incident investigation process follows the general objectives of investigation methodology, including:

- Conduct objective, thorough, and timely incident investigations
- Preserve individual privacy rights
- Collect, preserve, and protect incident/investigation data
- Maintain confidentiality as required
- Maintain thorough documentation of entire investigation process
- Safeguard investigation material/documentation
- Maintain chain of custody of investigation material/documentation
- Develop conclusions fully supported by facts in evidence
- Conduct a post-incident review of investigation, and document policy or procedural issues that enhanced or hindered the incident detection, monitoring, investigation, and subsequent development and implementation of corrective or problem bypass measures

11.1 Phase One - Identification and Assessment Steps

- Identify and verify problem (incident types and descriptions)
- Characterize the damage and extent of the problem, rate the incident severity Determine what investigation actions are to be taken
- Determine CSIRT resources are required to conduct the investigation, request/secure hardware, software, personnel resources
- Communicate with parties that need to be aware of the investigation

11.2 Phase Two - Containment and Eradication

- Collect and protect information associated with an incident investigation
- Contain the incident and determine further recovery or bypass actions to be taken
- Eliminate intruder's means of access and any related vulnerabilities

11.3 Phase Three - Recovery and Follow-up

- Return the systems to normal operations

- Close out the problem and follow up with a periodic post mortem review of the investigation.
- Prepare and publish report, as required.

If an incident has a rating of “high”, a brief formal report to UISAG through Director [ITeMS] shall be submitted upon closure of the incident. The report shall describe the incident, investigation methods, general conclusion, recommendations to avoid future related incidents and, if appropriate, lessons learned from the investigation.

12.0 INCIDENT TRACKING

The CSIRT will log, track and document the investigation and resolution of all security incidents. Where possible, software will be used to perform these functions.

The CSIRT supporting software will generate a trouble ticket within the "security schema," a set of forms containing customized fields and actions. The trouble ticket data for a particular incident investigation will only be available to the CSIRT members participating in the investigation. The trouble ticket data will not include any personally identifiable “confidential” information. Reports and summaries based on the data shall be generated as provided in the section on Incident Reporting.

13.0 INCIDENT REPORTING

A report showing all incidents related to service interruptions will be reviewed weekly during a CSIRT operational meeting. The purpose is to discover how serious the incident was, what steps are being taken to prevent reoccurrence, and if the root cause needs to be pursued.

The reports identified in this section will be generated from the incident tracking system. Where possible, these reports will be generated and distributed electronically:

Daily aging report: A daily report shall be sent via email to the CSIRT Chair on the status of the open tickets.

Monthly statistics report: A monthly report summarizing the incidents over the previous month shall be sent to Director, Information Technology and Media Services [ITeMS].

Quarterly statistics report: A quarterly report shall be forwarded to Director, Information Technology and Media Services [ITeMS] containing a summary of incidents investigated during the previous quarter. The quarterly report will also include an evaluation of incident trends, including popular entry methods, prevention tips, and new tools.

Real-time Alerts: As determined appropriate by the CSIRT Chair, alerts describing recent computer/network threats identified by CSIRT investigations and vulnerability prevention methods will be distributed on a timely basis. Such alerts may be distributed by web publications and/or other means, such as ebulletin.

13.1 Metrics

The following metrics should generally be used to produce the reports above. Metrics to be reported are:

- Total numbers of Incidents (as a control measure)
- Breakdown of incidents at each stage (e.g. logged, work in progress, closed etc)
- Size of current incident backlog
- Number and percentage of major incidents
- Mean elapsed time to achieve incident resolution or circumvention, broken down by impact code
- Percentage of incidents handled within agreed response time as defined by SLA’s or ISD standards
- Number of incidents reopened and as a percentage of the total
- Number and percentage of incidents incorrectly assigned
- Number and percentage of incidents incorrectly categorized
- Percentage of Incidents closed by the Service Desk without reference to other levels of support

(often referred to as 'first point of contact')
- Number and percentage of the incidents processed per CSIRT member
- Number and percentage of incidents resolved remotely, without the need for a visit
- Breakdown of incidents by time of day, to help pinpoint peaks and ensure matching of resources.

14.0 INCIDENT CLOSURE

Once the systems have been returned to normal operations, the CSIRT will verify that all corrective and/or preventive tasks are complete and that local services have been restored.

In cases where a department/unit external to ITeMS is responsible for incident resolution, the CSIRT Chair will monitor and document incident resolution. If an incident is rated as a "low" severity, the CSIRT Chair or an individual designated by the CSIRT Chair may close it. If an incident is rated with a "medium" severity, the CSIRT Chair must approve closure of the incident. If an incident has received a "high" severity rating, Director, Information Technology and Media Services [ITeMS] must approve closure of the incident. At any time the UISAG and/or the Vice Chancellor may terminate an incident investigation, regardless of incident severity rating.

If an incident is turned over to a law enforcement agency, the CSIRT incident investigation will, in most cases, be terminated.

15.0 BIBLIOGRAPHY

1. University of Scranton (2009). University of Scranton Computer Security Incident Response Team Operational Standards, Information Security Office 1/27/2009. Available at https://www.scranton.edu/pir/documents/CSIRT%20Operational%20Standards%20Manual.pdf

2. Hoepers, C. (2008) Incident Management and Computer Security Incident Response Teams (CSIRTs), 4th Caribbean Internet Governance Forum – Curaçao – July 24, 2008. Available at https://www.cert.br/docs/palestras/certbr-cigf2008.pdf

3. Cichonski, P.; Millar, T.; Grance, T. and Scarfone K. (2012). Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology. Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

4. University of British Columbia (2015). UBC Incident Response Plan. Available at https://it.ubc.ca/sites/it.ubc.ca/files/UBC_Incident_Response_Plan7600.pdf

5. European Union Agency for Network and Information Security (2006) CSIRT Setting Up Guide in English. Available at https://www.enisa.europa.eu/publications/csirt-setting-up-guide

6. Nigerian Cybercrime (Prohibition, Prevention, etc) Act 2015. Available at https://cert.gov.ng/images/uploads/CyberCrime_%28Prohibition%2CPrevention%2Cetc%29_Act%2C_2015.pdf

7. National Cybersecurity Strategy. (2014). Available at https://cert.gov.ng/images/uploads/NATIONAL_CYBESECURITY_STRATEGY.pdf

8. National Cybersecurity Policy. (2014). Available at https://cert.gov.ng/images/uploads/NATIONAL_CYBESECURITY_POLICY.pdf

9. AfricaCERT. Available at http://www.africacert.org/

INFORMATION ABOUT THE NIGERIAN NATIONAL CERT/CSIRT

Team Name	ngCERT
Official Team Name	Nigerian Computer Emergency Response Team
Date of membership approval	2015-07-31
Host organization	Office of National Security Adviser (ONSA)
Country of Team	Nigeria
Date of establishment	2015-02-01
Website	http://www.cert.gov.ng
Team contact information	
Regular telephone number	• +234-7044642378 • +234-8036594304 • +234-9-2904605 (fax) • +234-9-2904605
Emergency telephone number	+234-8036594304
E-mail address	incident@cert.gov.ng
Facsimile number	+234-9-2904605
Other communication facilities	ngCERT / Twitter : #ngCERT
Postal address	No. 26 Addis Ababa crescent, Wuse zone 4, Abuja, Nigeria
Business hours	
Timezone	GMT+1
Specification of business hours	08:00hrs - 18:00hrs
How to contact team outside business hours	+234 8036594304 (GMT+1:00)
Constituency	
Type of constituency	Government, Private and Public sectors
Source of constituency	Both external and internal
Description of constituency	ngCERT is recognized as the Nigerian National CSIRT in Nigeria, and as so, the referral agency that coordinates and facilitates the handling of incidents across the National Nigerian cyberspace, covering all the .ng Nigerian TLD, and all National IS
Internet domain address	.ng Nigerian TLD
Country of constituency	Nigeria
Cryptography	
PGP key id	0xB63CCD6F
PGP fingerprint	B3CF AD9E 3032 D6DF 0851 6763 C10D E32B B63C CD6F
Team PGP public key	

Source: https://www.first.org/members/teams/ngcert (accessed March 29, 2017)

TRAFFIC LIGHT PROTOCOL (TLP)
FIRST Standards Definitions and Usage Guidance — Version 1.0

1. Introduction

1. The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s). TLP only has four colors; any designations not listed in this standard are not considered valid by FIRST.
2. TLP provides a simple and intuitive schema for indicating when and how sensitive information can be shared, facilitating more frequent and effective collaboration. TLP is not a "control marking" or classification scheme. TLP was not designed to handle licensing terms, handling and encryption rules, and restrictions on action or instrumentation of information. TLP labels and their definitions are not intended to have any effect on freedom of information or "sunshine" laws in any jurisdiction.
3. TLP is optimized for ease of adoption, human readability and person-to-person sharing; it may be used in automated sharing exchanges, but is not optimized for that use.
4. TLP is distinct from the Chatham House rule (when a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.), but may be used in conjunction if it is deemed appropriate by participants in an information exchange.
5. **The source is responsible for ensuring that recipients of TLP information understand and can follow TLP sharing guidance.**
6. **If a recipient needs to share the information more widely than indicated by the original TLP designation, they must obtain explicit permission from the original source.**

2. Usage

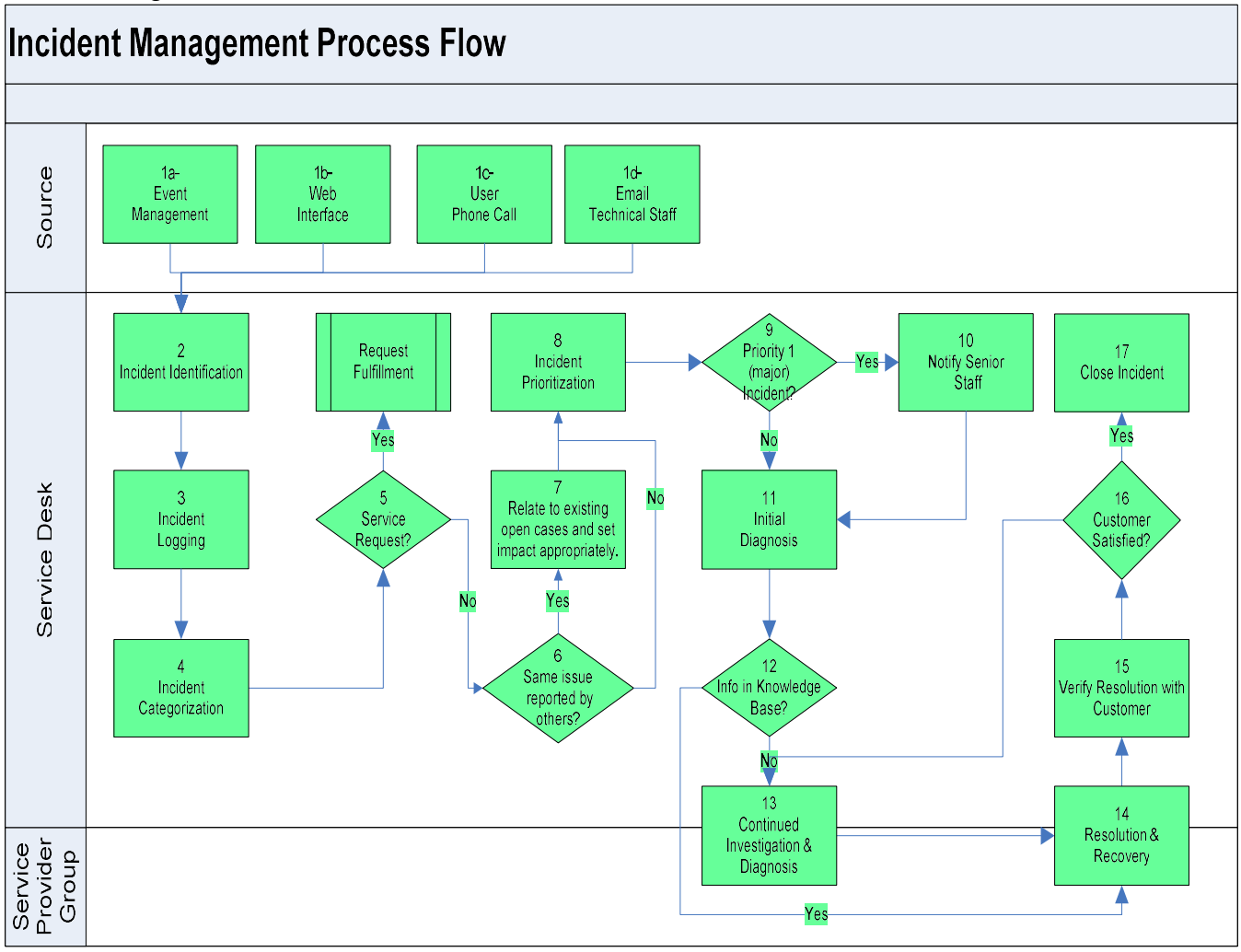
1. **How to use TLP in email**
   TLP-designated email correspondence should indicate the TLP color of the information in the Subject line and in the body of the email, prior to the designated information itself. The TLP color must be in capital letters: TLP:RED, TLP:AMBER, TLP:GREEN, or TLP:WHITE.
2. **How to use TLP in documents** TLP-designated documents should indicate the TLP color of the information in the header and footer of each page. To avoid confusion with existing control marking schemes, it is advisable to right-justify TLP designations. The TLP color should appear in capital letters and in 12 point type or greater.
   - **RGB**:
     TLP:RED : R=255, G=0, B=51, background: R=0, G=0, B=0 TLP:AMBER : R=255, G=192, B=0, background: R=0, G=0, B=0 TLP:GREEN : R=51, G=255, B=0, background: R=0, G=0, B=0 TLP:WHITE : R=255, G=255, B=255, background: R=0, G=0, B=0
   - **CMYK**:
     TLP:RED : C=0, M=100, Y=79, K=0, background: C=0, M=0, Y=0, K=100 TLP:AMBER : C=0, M=25, Y=100, K=0, background: C=0, M=0, Y=0, K=100 TLP:GREEN : C=79, M=0, Y=100, K=0, background: C=0, M=0, Y=0, K=100 TLP:WHITE : C=0, M=0, Y=0, K=0, background: C=0, M=0, Y=0, K=100

3. TLP definitions

1. **TLP:RED** = Not for disclosure, restricted to participants only.
   Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
2. **TLP:AMBER** = Limited disclosure, restricted to participants' organizations.
   Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

3. **TLP:GREEN** = Limited disclosure, restricted to the community.
   Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not released outside of the community.
4. **TLP:WHITE** = Disclosure is not limited.
   Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Incident Management Processes



Membership of University of Ibadan CSIRT (UI-CSIRT)

Vice-Chancellor	
Director, ITeMS	
Security Manager / CSIRT Chair	Deputy Director, Information Technology, Network and Hardware
University Information Security Advisory Group = Board of ITeMS	
Chairman	
Head, Computer Science Head, Electrical/Electronics	
Senate Representative 1	
Senate Representative 2	
Representative of Registrar	
Representative of Bursar	
Representative of University Librarian	
Representative of University Health Services	
Representative of PG School Representative of Distance learning Centre	
Representative of CESDEV	
Representative of CEI	
Representative of College of Medicine	
Representative of UI Business School	
Director, Physical Planning	
Director, Quality Assurance	
Director, Works and Maintenance	
Independent members (4)	
Core Team	
Hardware/Network	
Software/Programming	
E-mail Administrator	
Web master **Support/Technical Team**	
Network Administrators	
Systems Analyst	
3rd Party Service Providers	Onet, IPNX, SocketWorks