CERT-PH Incident Reporting and Technical Assistance Request Guidelines

Version 1.0

CERT-PH
NATIONAL COMPUTER EMERGENCY RESPONSE TEAM
DICT

Table of Contents

I. Purpose

The purpose of this document is to provide guidelines to the different agencies, CERTs, stakeholders, and External Information Sharing and Analysis Organizations in submitting incident reports and requesting for cybersecurity related technical assistance to the National Computer Emergency Response Team (CERT-PH).

II. Objectives

These guidelines support CERT-PH in executing its mission objectives and enable the following benefits:

- Provide greater quality of information
- Improve information sharing process
- Provide agile and effective incident response

III. Incident Report and Technical Assistance Request Requirement

Cybersecurity incidents that potentially affect or compromise the confidentiality, integrity, or availability of the information system must be reported to the National Computer Emergency Response Team (CERT-PH). Incident reports that do not have confirmed functional or information impact such as passive scan, phishing attempts, attempted access, or thwarted exploits may be submitted to CERT-PH voluntarily. All incident reports submitted to CERT-PH must use the appropriate CERT-PH Report Template and must be filled out with the required essential data and other relevant information available.

Cybersecurity related technical assistance request must use the appropriate CERT-PH Technical Assistance Request Form and must be filled out with the required essential data and other relevant information available. Technical assistance that CERT-PH can provide to the stakeholders will be limited to the core services that is being offered. These includes incident response support, cyber threats monitoring and investigation.

Reporting an incident to the CERT-PH must adhere to the recommended report timeframe in Cyber Threat Level Indicator and provide all available information. The recommended report timeframe must be followed in order to address the incident rapidly and to provide further details (i.e. root cause, vulnerabilities exploited, or mitigation actions taken) as this may result in high risk to the system. Reporting agencies/stakeholders may provide other information in addition to the submitted report in support of the ongoing investigation by CERT-PH.

IV. Reporting an Incident

Incident reports and notifications sent to CERT-PH must follow the appropriate report form template. The information elements described below are required in submitting an incident or notification report: (Refer to Annex A and B to see the report form templates.)

- **Submitting an Incident Report Form**

The information elements described in steps 1-14 below are the key data elements needed when notifying CERT-PH of an incident:

1. Provide an Incident Name for the report. **required*
2. Indicate the date of your report. **required*
3. Indicate the Name of the reporter. **required*
4. Input the reporters contact number. **required*
5. Input the reporters email address. **required*
6. Indicate the Agency/Division/Bureau affected by the incident. **required*
7. Identify the targeted assets affected by the incident. **required*
8. Indicate the source/s of information relevant to the incident.
9. Indicate the appropriate Traffic Light Protocol for the incident. (Refer to Annex C to see the appropriate TLP.)
10. Provide a brief summary of the incident. **required*
11. Identify the current level of impact on agency functions or services (Functional Impact).
12. Identify the type of information lost, compromised, or corrupted (Information Impact).
13. Estimate the scope of time and resources needed to recover from the incident (Recoverability).
14. Indicate the action/s taken at the time of discovery of the incident. **required*

The following information should also be included if known at the time of submission:

- Identify the attack vector(s) that led to the incident.
  - (Refer to Table 5 to see the Attack Vector Taxonomy)
  - (Refer to Table 6 to identifying the appropriate vector)
- Provide any indicators of compromise, including signatures or detection measures developed in relation to the incident.
- Provide any mitigation activities undertaken in response to the incident.

Reports must be submitted using the CERT-PH Incident Report Template and must be sent to cert-ph@dict.gov.ph.

Important: Sensitive and personal information submitted and inputted through the forms are collected and handled according to and in compliance with the Republic Act 10173 – Data Privacy Act of 2012.

V. Impact and Severity Assessment

Assessment of the impact and severity of an incident will be the baseline of the prioritization. Incident reports will be prioritized based on the relevant factors, such as the following:

- **Functional Impact of the Incident.**

  Incidents targeting IT systems typically impact the business functionality that those systems provide, resulting in some type of negative impact to the users of those systems. Incident handlers should consider how the incident will impact the existing functionality of the affected systems. Incident handlers should consider not only the current functional impact of the incident, but also the likely future functional impact of the incident if it is not immediately contained.

- **Information Impact of the Incident.**

  Incidents may affect the confidentiality, integrity, and availability of the organization's information. For example, a malicious agent may exfiltrate sensitive information. Incident handlers should consider how this information exfiltration will impact the organization's overall mission. An incident that results in the exfiltration of sensitive information may also affect other organizations if any of the data pertained to a partner organization.

- **Recoverability from the Incident.**

  The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident. In some instances it is not possible to recover from an incident (e.g., if the confidentiality of sensitive information has been compromised) and it would not make sense to spend limited resources on an elongated incident handling cycle, unless that effort was directed at ensuring that a similar incident did not occur in the future. In other cases, an incident may require far more resources to handle than what an organization has available. Incident handlers should consider the effort necessary to actually recover from an incident and carefully weigh that against the value the recovery effort will create and any requirements related to incident handling.

- **Cyber Threat Level Indicator**

Table 1: Cyber Threat Level Indicator

Color Indicator	Threat Level	Description	Report Timeframe
RED (rating 9-11)	Critical	Ransomware, C&C Server, DDOS affecting all critical sectors, Data breach with critical information exposed, wide-spread destructive compromised system, 0-day, Supply Chain attacks	12 hours upon discovery of the incident
ORANGE (rating 6-8)	High	Compromised executive email, Malware infiltration, Network and system Intrusion	18 hours upon discovery of the incident
YELLOW (rating 4-5)	Elevated	Detected known vulnerabilities, Idle botnets and backdoors, Unresolved signs of system intrusion(website defacements, etc.)	24 hours upon discovery of the incident

BLUE (rating 2-3)	Moderate	Phishing Incidents, Compromised systems/websites with non-sensitive information	48 hours upon discovery of the incident
GREEN (0-1)	Low	Unverified Anomalies	48 hours upon discovery of the incident

VI. Impact Category Descriptions

The following tables define each impact category description and its associated severity levels. Use the tables below to identify impact levels and incident details.

A. Functional Impact Guide

A measure of the impact to business functionality or ability to provide services.

Table 2: Functional Impact Guide

Category Rating		Definition
0	**NONE**	No effect to the organization's ability to provide all services to all users
1	**LOW**	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency *(or may happen based on the nature of cyber-attack)*
2	**MEDIUM**	Organization has lost the ability to provide a critical service to a subset of system users *(or may happen based on the nature of cyber-attack)*
3	**HIGH**	Organization is no longer able to provide some critical services to any users *(or may happen based on the nature of cyber-attack)*

B. Information Impact Guide

Describes the type of information lost, compromised, or corrupted.

Table 3: Information Impact Guide

Category Rating		Definition
0	**NONE**	No information was exfiltrated, changed, deleted, or otherwise compromised
1	**INTEGRITY**	Integrity Loss; Sensitive or was changed or deleted *(or may happen based on the nature of cyber-attack)*
2	**PRIVACY**	Privacy Breach; Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated *(or may happen based on the nature of cyber-attack)*
3	**PROPRIETARY**	Proprietary Breach; Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated

		(or may happen based on the nature of cyber-attack)
4	**CLASSIFIED**	The confidentiality of classified information was compromised. *(or may happen based on the nature of cyber-attack)*

C. **Recoverability Effort Rating Guide**

Identifies the scope of resources needed to recover from the incident.

Table 4: Recoverability Effort Rating Guide

Category Rating		Definition
0	**NOT APPLICABLE**	Incident does not require recovery.
1	**REGULAR**	Regular; Time to recovery is predictable with existing resources
2	**SUPPLEMENTED**	Supplemented; Time to recovery is predictable with additional resources
3	**EXTENDED**	Extended; Time to recovery is unpredictable; additional resources and outside help are needed
4	**NOT RECOVERABLE**	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

Ref: NIST Special Publication 800-61 - "Computer Security Incident Handling Guide"

This information will be utilized to calculate a severity score and priority threat level according to the CERT-PH Cyber Threat Level Indicator.

- **Critical** (**Red**) - Severity and Priority Threat Level score ranging from 9-11.
- **High** (**Orange**) - Severity and Priority Threat Level score ranging from 6-8.
- **Elevated** (**Yellow**) - Severity and Priority Threat Level score ranging from 4-5.
- **Moderate** (**Blue**) - Severity and Priority Threat Level score ranging from 2-3.
- **Low** (**Green**) - Severity and Priority Threat Level score ranging from 0-1.

VII. Attack Vectors

This document shares its attack vector terminologies to various organizations in order to adopt a common set of terms and relationships. The attack vectors categories are not intended to provide definitive classification for incidents; rather, they simply list common methods of attack, which can be used as a basis for defining more specific handling procedures. All Government CERTs are required to use the following taxonomy and apply it in sending cybersecurity related incidents or notifications.

A. Attack Vectors Taxonomy

Table 5: Attack Vectors Taxonomy

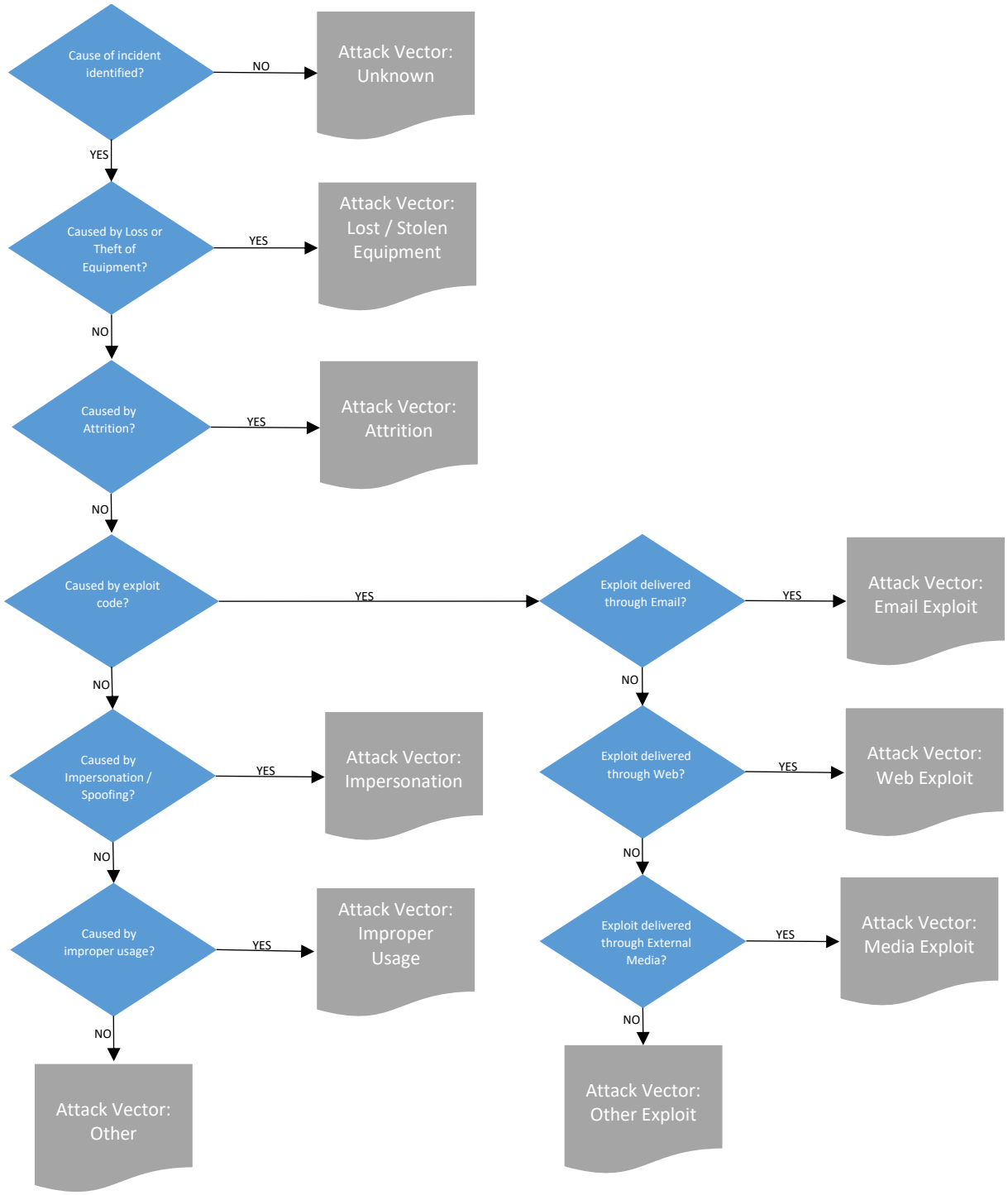
Attack Vector	Description	Example
Unknown	Cause of the attack is unidentified.	This option is acceptable if cause (vector) is unknown upon initial report. The attack vector may be updated in a follow-up report.
Attrition	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.	Denial of Service intended to impair or deny access to an application; a brute force attack against an authentication mechanism, such as passwords or digital signatures.
Web	An attack executed from a website or web-based application.	Cross-site scripting attack used to steal credentials, or a redirect to a site that exploits a browser vulnerability and installs malware.
Email/Phishing	An attack executed via an email message or attachment.	Exploit code disguised as an attached document, or a link to a malicious website in the body of an email message.
External/Removable Media	An attack executed from removable media or a peripheral device.	Malicious code spreading onto a system from an infected flash drive.
Impersonation/ Spoofing	An attack involving replacement of legitimate content/services with a malicious substitute.	Spoofing, man in the middle attacks, rogue wireless access points, and structured query language injection attacks all involve impersonation.
Improper Usage	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.	User installs file-sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization.	A misplaced laptop or mobile device.
Other	An attack method does not fit into any other vector	

Ref: US-CERT - "US-CERT Federal Incident Notification Guidelines"

B. Cause Analysis

Table 6: Cause Analysis Diagram

The diagram below will be the guide in identifying the appropriate vector:



Ref: US-CERT - "US-CERT Federal Incident Notification Guidelines"

VIII. Requesting for a Cybersecurity Technical Assistance

Cybersecurity related technical assistance request must use the appropriate CERT-PH Technical Assistance Request Form and must be filled out with the required essential data and other relevant information available. Technical assistance that CERT-PH can provide to the stakeholders will be limited to the core services that is being offered. These includes incident response support, cyber threats monitoring and investigation**.**

- **Submitting a Technical Assistance Request Form**

The information elements described in steps 1-11 below are the key data elements needed when notifying CERT-PH of an incident:

1. Provide a technical assistance request title. **required*
2. Indicate the date of your request. **required*
3. Indicate the name of the person requesting. **required*
4. Input the requestors' contact number. **required*
5. Input the requestors' email address. **required*
6. Indicate the Agency/Division/Bureau requesting for assistance. **required*
7. Indicate the appropriate Traffic Light Protocol for the incident. (Refer to Annex C to see the appropriate TLP.)
8. Provide a brief summary of the incident. **required*
9. Indicate the objective of the request. **required*
10. Include necessary information/artifacts needed. **required*
11. Indicate the action/s to be taken in the technical assistance being requested. **required*

Reports must be submitted using the CERT-PH Incident Report Template and must be sent to cert-ph@dict.gov.ph.

Important: Sensitive and personal information submitted and inputted through the forms are collected and handled according to and in compliance with the Republic Act 10173 – Data Privacy Act of 2012.

ANNEX

A. CERT-PH Incident Report Form Template:

CERT-PH Incident Report Form	
Incident:	*(Data element is required)*
Report Date:	*(Data element is required)*
Reporter Name:	*(Data element is required)*
Contact Number:	*(Data element is required)*
Email:	*(Data element is required)*
Agency / Division / Bureau	*(Data element is required)*
Targeted Assets	*(Data element is required)*
Information Source	
TLP: _____	**(Refer to Annex C to determine the appropriate TLP)**

Incident Description/ Details
(Data element is required)

Threat Vectors/ Incident type/ Description
(Refer to Table 6 to identify appropriate attack vector)

Impact Classification
Functional: (Refer to Table 2 to identify appropriate category rating)
Informational: (Refer to Table 3 to identify appropriate category rating)
Recoverability: (Refer to Table 4 to identify appropriate category rating)

Description of Actions Taken at the time of discovery
(Data element is required)

B. CERT-PH Technical Assistance Request Form Template:

CERT-PH Technical Assistance Request Form	
Request Title:	*(Data element is required)*
Request Date:	*(Data element is required)*
Requested by:	*(Data element is required)*
Contact Number:	*(Data element is required)*
Email:	*(Data element is required)*
Agency / Division / Bureau	*(Data element is required)*
TLP: _____	**(Refer to Annex C to determine the appropriate TLP)**

Technical Assistance Request Description
(Data element is required)

Objective of Request
(Data element is required)

Attached additional Information / Artifacts
(Data element is required)

Requested Technical Assistance to be Performed
(Data element is required)

C. Traffic Light Protocol (TLP)

Color	When it should be used?	How it may be shared?
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.
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.
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 be released outside of the community.
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.