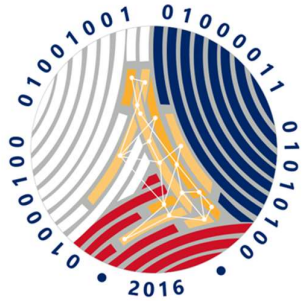
# CERT-PH

NATIONAL COMPUTER EMERGENCY RESPONSE TEAM




DICT

# Table of Contents

# 1. Document Information

This document contains a description of CERT-PH in accordance with the RFC 2350[1]. In addition, it provides basic information about the CERT-PH, its communication channels, and the services it offers.

## 1.1. Date of Last Update

Version 1.0 - 2020/04/21

Version 2.0 – 2022/08/26

Version 3.0 - 2023/04/13

## 1.2. Distribution List for Notifications

There is no distribution list for notifications.

## 1.3. Locations where this Document May Be Found

The current version of this document can always be accessed at www.ncert.gov.ph.

## 1.4. Authenticating This Document

This document has been signed with the CERT-PH PGP key.

# 2. Contact Information

## 2.1. Name of the Team

Philippine National Computer Emergency Response Team (CERT-PH)

## 2.2. Address

Cybersecurity Bureau Building
Department of Information and Communications Technology
49 Don A. Roces cor. Sct. Reyes
Diliman, Quezon City

## 2.3. Time Zone

(UTC +08:00) Manila, Philippines

## 2.4. Telephone Number

CERT-PH Hotline Number: (+632) 8920-0101 local 2378 (CERT)

## 2.5. Facsimile Number

Not Available

## 2.6. Other Telecommunication

Facebook: https://www.facebook.com/Ncertgovph

## 2.7. Electronic Mail Address

CERT-PH Email Address: cert-ph@dict.gov.ph

## 2.8. Public Keys and Encryption Information

Bits: 4096
ID : 4E4870031D742ECF
Key Fingerprint : 3F24 F8C4 B43D E74A 2410 2E13 4E48 7003 1D74 2ECF

[1] Expectations for Computer Security Incident Response (https://www.rfc-editor.org/rfc/pdfrfc/rfc2350.txt.pdf)

### 2.9. Team Members

The team comprises information security analysts, information officers, and engineers from the National Computer Emergency Response Team division under the Cybersecurity Bureau of the Department of Information and Communications Technology - Philippines.

### 2.10. Other Information

Further information about CERT-PH can be found at https://www.ncert.gov.ph.

### 2.11. Points of Customer Contact

The preferred method for contacting CERT-PH is via email. For incident reports and related issues, use cert-ph@dict.gov.ph. This email is monitored regularly, and emails will be acted upon once received.

CERT-PH hours of operations are usually restricted to regular business hours (07:00 – 18:00 Monday to Friday). However, for out-of-business hours support in case of critical security incidents, CERT-PH is available on on-call duty.

## 3. Charter

### 3.1. Mission Statement

CERT-PH is responsible for receiving, reviewing, and responding to computer security incident reports and activities. The team also ensures that systematic information gathering/dissemination, coordination, and collaboration among stakeholders, especially computer emergency response teams, are maintained to mitigate information security threats and cybersecurity risks.

### 3.2. Constituency

Stipulated in the DICT Department Circular 003[2], CERT-PH, the national CERT of the Philippines, shall lead, manage, and oversee the various Government, Sectoral and Organizational CERTs within the Philippines.

### 3.3. Sponsorship and/or Affiliation

CERT-PH is established within the Cybersecurity Bureau of the Department of Information and Communications Technology, Philippines.

CERT-PH is recognized under the Software Engineering Institute (SEI) Division at Carnegie Mellon University. In addition, it is currently affiliated with the ASEAN-Japan Cybersecurity Working Group, is an Operational Member of the Asia Pacific Computer Emergency Response Team (APCERT), and an Operating Committee Member of the Cybersecurity Alliance for Mutual Progress (CAMP).

### 3.4. Authority

CERT-PH is mandated to provide pro-active government countermeasures to address and anticipate all domestic and transnational incidents affecting the Philippine cyberspace and any cybersecurity threats to the country.

## 4. Policies

### 4.1. Types of Incidents and Level of Support

Cybersecurity incidents that potentially affect or compromise the information system's confidentiality, integrity, or availability must be reported to 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. The level of support given by CERT-PH will vary depending on the type and severity of the incident, the constituent and/or constituents impacted, and available resources.

[2] DICT Department Circular 003 – Supplementing the DICT Memorandum Circular Nos. 005, 006, 007, Series of 2017, and Policies, Rules and Regulations on the Implementation of the National Cybersecurity Plan 2022

### 4.2. Co-operation, Interaction, and Disclosure of Information

CERT-PH values the privacy of all the concerned and affected agencies, organizations, and clients that have been accommodated by the team as much as we value their security. Disclosure of information is in accordance with Philippine Republic Act No. 10173 or the Data Privacy Act of 2012 and in conformance with other issuances of the National Privacy Commission. To ensure that information is shared only with the appropriate audience or recipient, CERT-PH utilizes the Traffic Light Protocol (TLP)[3] for information sharing.

### 4.3. Communication and Authentication

Communication via email is preferred and in situations where highly sensitive information is exchanged, usage of PGP/GPG is supported. CERT-PH is also reachable by telephone.

## 5. Services

### 5.1. Incident Response

CERT-PH's incident response services are available on a 24/7 basis to its constituency. All information and communication technologies related incidents are evaluated.

#### Incident Triage

- Determine whether an incident is authentic;
- Assess the impact and priority of the incident

#### Incident Coordination

- Contact the involved parties to investigate the incident and take the appropriate steps;
- Determine the possible cause of the incident;
- Facilitate contact with other parties, which can help resolve the incident

#### Incident Resolution

- Provide technical recommendations for post-incident recovery
- Provide technical recommendations to correct system vulnerabilities
- Provide Mobile Security Operation Center to monitor, analyze and understand on-going cyber attacks

### 5.2. Proactive Service

#### Threat Monitoring and Information Sharing

- Monitor, collect and analyze cybersecurity threats;
- Provide vulnerability reports to affected agencies
- Issue corresponding threat feeds and advisories on the latest cybersecurity related topics

#### Vulnerability Assessment and Penetration Testing

- Conduct Vulnerability Assessment and Penetration Testing to Government Agencies and Instrumentalities, and Identified Critical Information Infrastructure (CIIs);
- Examine and evaluate web and mobile applications, and network assets to identify security deficiencies;
- Provide visibility of security flaws and weaknesses to system owners by presenting the technical details and analysis of the discovered vulnerabilities and its corresponding criticalities.
- Provide solutions and recommendations based on the assessment findings to ensure the integrity and security of organization's systems, consequently improving their cyber security posture.
- Provide technical details and analysis of discovered vulnerabilities and criticality to systems owner;
- Recommend steps based on the assessment results to improve the organization’s security posture.

[3] Forum of Incident Response and Security Teams (FIRST) Standard Definitions and Usage Guidance (https://www.first.org/tlp/)

### Education / Training

- Conduct cybersecurity trainings for technical and non-technical officers from the public sector
- Conduct CSIRT operations and other CSIRT related trainings

## 6. Incident Reporting Forms

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.

## 7. Disclaimer

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