Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
INFORMATION TECHNOLOGY MANAGEMENT SERVICE
Camp Crame, Quezon City

Computer Security Incident Reporting Form

Instructions: This form is to be completed as soon as possible following the detection or reporting of an Information Technology (IT) / Computer security incident within PNP offices and PNP property computer resources. All items completed should be based on information that is currently available.

1. Contact Information for this Incident	
Rank/Name:	
Designation:	
PNP Office:	
Work Phone:	
Mobile Phone:	
Email address:	
Fax Number:	

2. Incident Description.

Provide a brief description:

3. Impact / Potential Impact Check all of the following that apply to this incident.

- ☐ Loss / Compromise of Computer Data
- ☐ Damage to Computer Systems
- ☐ System Downtime / Unavailability of Service
- ☐ Financial Loss
- ☐ Other Offices' Systems Affected
- ☐ Damage to the Integrity or Delivery of Critical Services or Information
- ☐ Violation of PNP Policies / Government Regulations / Philippine Laws
- ☐ Unknown at this time

Provide a brief description:

4. Sensitivity of Data/Information Involved Check all of the following that apply to this incident.

Sensitivity of Data	
Category	**Example**
Public	This information has been specifically approved for public release. Unauthorized disclosure of this information will not cause problems for the PNP, its customers, Data Privacy Law, Police operations/investigations or National Security.
Internal Use Only	This information is intended for use within the PNP or between agencies, and in some cases within accredited organizations. Unauthorized disclosure of this information to outsiders may be against laws and regulations, or may cause problems for the PNP. This type of information is already widely distributed within the PNP, or it could be so distributed within the organization without advance permission from the information owner.
Restricted/Confidential (Privacy Violation)	This information is private or otherwise sensitive in nature and must be restricted to those with authorized access. Unauthorized disclosure of this information to people without authority for access may be against laws and regulations, or may cause significant problems for the PNP, its customers. Decisions about the provision of access to this information must be cleared through the information owner.
Unknown/Other	Describe in the space provided

☐ Public ☐ Internal Use Only	☐ Restricted / Confidential (Privacy violation) ☐ Unknown / Other – please describe:

Provide a brief description of data that was compromised:

5. Who Else Has Been Notified?

Provide Rank/Name and Title/Designation:

6. What Steps Have Been Taken So Far? Check all of the following that apply to this incident.

☐ No action taken ☐ System Disconnected from network	☐ Restored backup from external storage device

☐ Updated virus definitions & scanned system	☐ Log files examined (saved & secured) ☐ Other – please describe:
Provide a brief description:	

7. Incident Details	
Date and Time the Incident was discovered:	
Has the incident been resolved?	
Physical location of affected system(s):	
Number of sites affected by the incident:	
Approximate number of systems affected by the incident:	
Approximate number of users affected by the incident:	
Are non-PNP computer systems affected by the incident? (Y or N – if Yes, please describe)	
Please provide any additional information that you feel is important but has not been provided elsewhere on this form.	

Please submit this completed form to:
wscsditms@pnp.gov.ph

For inquires call Web Services and Cyber Security Division, ITMS, PNP at 7230401 local 4225. This form may be updated, modified and reproduced. You can download the form at PNP ITMS website: http://www.itms.pnp.gov.ph