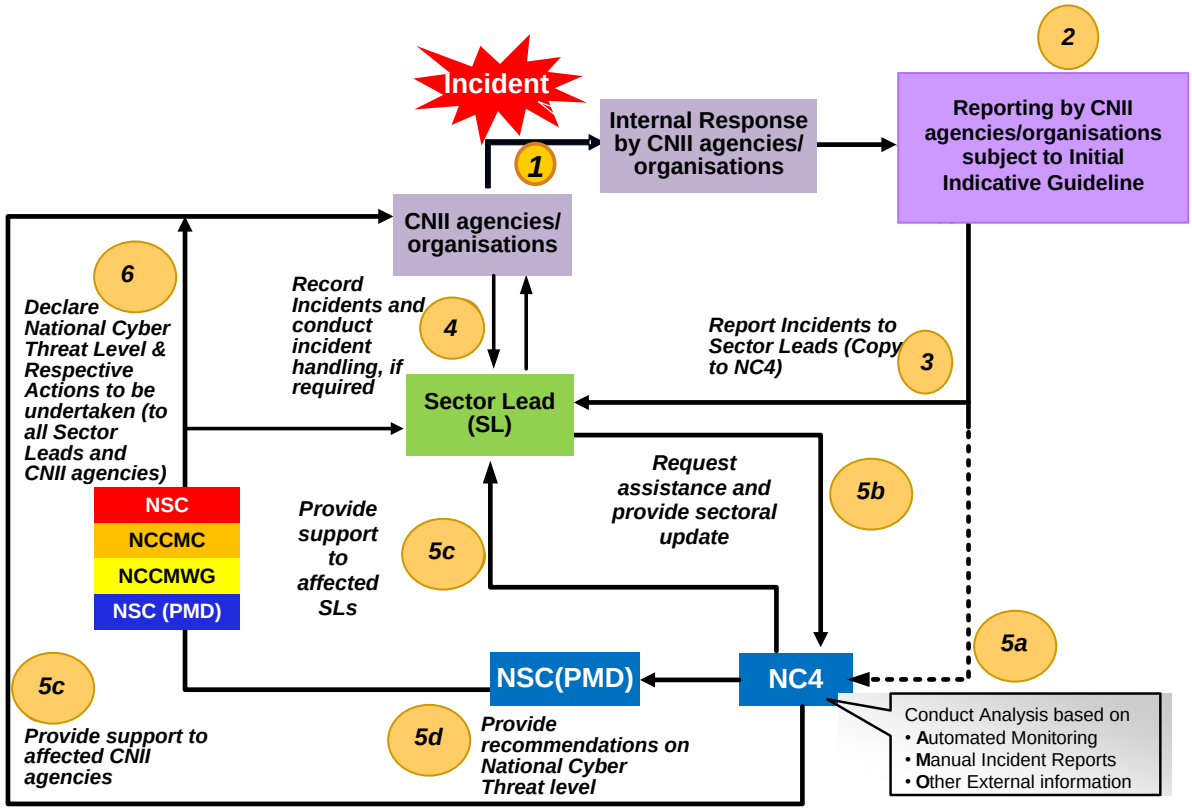
NATIONAL SECURITY COUNCIL

NATIONAL SECURITY COUNCIL

NATIONAL CYBER CRISIS MANAGEMENT

HIGH LEVEL OVERVIEW



High Level Overview Diagram

Note:
The numbers listed above indicate the sequence of processes that should take place after a cyber incident occurs at CNII agencies / organisations.

Description of High Level Overview Diagram

STEP	PROCESS
1	When an incident detected in CNII agencies / organisations, their CERT team would conduct their own response by identifying, containing and eradicating the incident at localized organisational level.
2	CNII agencies / organisations would determine if the incident warrants a report to their respective Sector Leads (SL) and based on Initial Indicative Guideline (as in **Appendix 1**)
3	(i) If reporting is required, affected CNII agencies / organisations will compile the required information and submit the Incident Reporting Form to respective SL and copy to NC4 as follows: (a) **Incident Reporting Form as in Appendix 2** is for all CNII Agencies/ Organisations that have been listed under 9 CNII sectors including government agencies/organisations under these sectors & Polytechnic and IPTA where Ministry of Higher Education will play role as Sector Lead. (b) **MAMPU's Incident Reporting Form** is for all CNII agencies/organisations that have been listed under another 1 CNII sector (other than 9 sectors above) i.e. Government Sector.
4	Relevant SLs would record incident and do necessary incident handling if incident was escalated by affected CNII agencies / organisations.
5a	Upon receiving information of reported incident, NC4 start doing monitoring taking into account other sources of information.
5b	If problems were not resolved at sector level, incidents would be escalated to NC4. At this stage: (i) NC4 would provide assistance to resolve incidents escalated by affected SLs; and (ii) Relevant SLs would continuously provide situational update to NC4
5c	NC4 would continuously provide support and assistance to affected CNII agencies / organisations and SLs.
5d	NC4 would provide situational update and recommendation on National Cyber Threat Level with associated action plans to National Security Council, Prime Minister's Department (NSC, PMD) accordingly.

STEP	PROCESS
6	NSC would decide on the National Cyber Threat Level. NSC would request for meeting to be convened in accordance with threat level that has been decided. National Cyber Threat Level will be declared by chairman of respective meeting session as follows: (a) Secretary of NSC (PMD) will chair the meeting when threat level is Moderate (Blue); (b) Secretary of NSC (PMD), who is also the Chairman of NCCMWG will chair the NCCMWG meeting when threat level is Caution (Yellow); (c) Minister of the Prime Minister's Department, the Chairman of NCCMC will chair the NCCMC meeting when threat level is High (Orange); and ~~(d)~~ Most Honourable Prime Minister, the Chairman of NSC will chair NSC Meeting when threat level is Critical (Red).

NATIONAL SECURITY COUNCIL

NATIONAL CYBER CRISIS MANAGEMENT

APPENDICES

Appendix 1: Initial Indicative Guideline for Reporting Cyber Incident

No.	Incident Type	Description / Example	Symptoms
1	**Denial of Service (DoS)/ Distributed Denial of Service (DDoS)**	A denial of service (DOS) attack is an incident in which a user or organisation is deprived of the critical services. In a distributed denial-of-service, large numbers of compromised systems (sometimes called a botnet) attack a single target.	(i) Unavailability of at least one (1) of critical services identified
2	**Intrusion**	Intrusion is referred to the unauthorised access or illegal access to a system or network, successfully. This could be the act of root compromise, web defacements, installation of malicious programs, i.e. backdoor or Trojan.	(i) Inaccessible/hacked of critical system accounts (ii) Classified information leakage (iii) Webs defacement (iv) Official email address being compromised to send spam
3	**Malicious Codes - Malware**	Malware, short for malicious software, is software designed to infiltrate a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. The term "computer virus" is sometimes used as a catch-all phrase to include all types of malware, including true viruses.	(i) Malware that affect critical system (ii) Spread of malware that cause disrupt of operations
4	**Malicious**	Definition of Malware hosting	(i) Users report getting

No.	Incident Type	Description / Example	Symptoms
	Codes-Malware Hosting	is where the malware reside whether at a compromised server or client PC that has been infected by virus/malware. Malicious software that is installed on a user's machine without their consent.	viruses from your web pages (ii) Notification from other parties (eg. notification from MyCERT, GCERT) (iii) Own monitoring and scanning
5	**Intrusion Attempt**	Attempts with intention to compromise a system. This is done through port scanning, login brute force and vulnerabilities probes.	(i) Alerts notification to the System Administrator from perimeter defense systems i.e. IDS, firewalls, SIEM (ii) Reports from third parties regarding the attempts (iii) Detection of anomalies activities by the System Administrator

Appendix 2: Incident Reporting Form

INCIDENT REPORTING FORM **Fields marked with an asterisk (*) are mandatory and must be completed**				
*Date & Time of Report:		Incident Ref No (Issued by National Cyber Coordination & Control Centre (NC4)):		
1. Contact information for this Incident				
***Name:**	***Organisation.:**			
***Office/Mobile No:**	***Email:**	**Fax No:**		
2. *Date and Time Incident Occurred				
3. *Type of Incident (tick all that apply)				
☐ Denial of Service (DoS)/ Distributed Denial of Service (DDos) ☐ Intrusion ☐ Malicious Code – Malware ☐ Malicious Code – Malware Hosting ☐ Intrusion Attempt				
*Please provide a description of the Incident:				
List of symptoms on the occurred incident:				
4. Information on Affected System:				
***IP Address (Range):**	**Computer/Host Name:**	***Operating System (including release number)**	**Other Applications**	**Critical System (YES/NO)**
				☐ Yes ☐ No
				☐ Yes ☐ No
				☐ Yes ☐ No
				☐ Yes ☐ No
5. *Number of host(s) affected:				
☐ 1 to 50	☐ 50 to 100	☐ 100 to 1000	☐ More than 1000	
6. IP Address of apparent or suspected source (if available):				
Source IP address:		Other Information Available:		

7. Additional Information:
If this incident is related to a previously reported incident, include any previously assigned incident number for reference:
Please attach any evidence – logs, artefacts (if available)
Any other comments or information that you wish to provide: