NIC- Computer Emergency Response Team (CERT)

Information Security Incident Management Policy

Document Control

Document Title	Information Security Incident Management Policy
Document Type	Policy Draft
Document Identifier	ISIMP
Version	1.0
Date of Release	November -2017
Document Owner	NIC-CERT
Document Author	HARIHARAN M
Document Reviewed By	Nagendra Kumar, HoD, NIC-CERT
Document Approved By	R.S.Mani, HoG, NIC-CERT

Document Change History

Version No.	Revision Date	Nature of Change	Date of Approval

Table of Contents

1. Information Security Incident Management Policy

1.1 Introduction

National Informatics Centre – Computer Emergency Response Team (NIC-CERT) Division, was constituted with an objective of acting as a single point of contact for responding, reporting and managing the following – information security incidents, vulnerabilities, advisories and co-ordinate with multiple stakeholders (like CERT-In, sectoral/state CERTs, Ministries, NIC Divisions, NIC State Units, Government Departments, Public Sector Units, Educational Institutions, Private Agencies/System Integrators/Contractors /OEMs / Vendors…etc) for information security related matters.

1.2 Purpose

The purpose of this policy is to ensure that all NIC employees, contractual staffs, Vendors and other stakeholders are fully aware and understand, the necessary process to be followed in case of an Information Security Incident and also to ensure that all Information Security incidents are duly reported to NIC-CERT and the same is documented and recorded.

1.3 Scope

This Policy is applicable to all NIC Employees, temporary/contractual staffs, Vendors, Third Party Personnel, Central and State Government Employees and other stakeholders who are using or accessing NIC's network or services.

2. Policy Statement

Any information security compromise/breach, attempt to compromise/breach, presence of security vulnerability/loop hole, violation of security policies/guidelines, leak/unauthorized access of data/systems, shall be reported to NIC-CERT immediately upon detection and the same shall be responded to by NIC-CERT as per this policy.

3. Information Security Incident Identification

An Information Security Incident is any event which threatens or has the potential to adversely affect the Confidentiality or Integrity or Availability, of the information systems/services, of NIC. Some of the examples of an Information Security Incidents includes but not limited to the following:

3.1 Website Defacement
3.2 Denial of Service (DoS) or Distributed Denial of Service (DDoS)
3.3 Unauthorized access or modification of Data or network or systems or services or programs
3.4 Violation of NIC's policies, processes, guidelines..etc.
3.5 Violation of Legal statutes and regulations (like IT Act, Aadhaar Act…etc)
3.6 Loss or Theft of equipment on which data is stored (Ex: Hard Disk, Removable Media, Servers….etc)
3.7 Social Engineering (Ex: Phishing, Spam, spoofing tele-calls…etc)
3.8 Advanced Persistent Threats
3.9 Ransomware Infection
3.10 Malware/Virus/Trojan/Worm – Outbreak
3.11 Data Exfiltration (Unauthorized Copying/Transferring, of data to external network/internet)
3.12 Hacking/Intrusion
3.13 Disclosure of sensitive data in public domain (Ex: display of personal information of citizens like bank records, date of birth….etc., in public domain)
3.14 Unauthorized Scanning (both horizontal and vertical) of NIC's network

4. Information Security Incident Reporting

4.1 If any user detects or observes any of the (but not limited to) Information Security incidents mentioned in Section 3, of this Policy. Then the same shall be reported by him/her, to NIC-CERT immediately.

4.2 Information Security incidents can be reported to NIC-CERT through any one of the following 3 Options:

Option 1:

Contact the 24x7, Toll Free number of NIC-CERT Helpdesk at:

011-22900-350

Option 2:

Write a brief description of incident, along with your contact details and send the same to NIC-CERT's incident response e-mail id:

Incident@nic-cert.nic.in

If necessary, send by e-mail the filled-up incident reporting form available at NIC-CERT's website:

https://nic-cert.nic.in/NIC_CERT_1/policies.jsp

Method 3:

Create a ticket at NIC's Service Desk, select category as security incident and fill-up the required details.

https://servicedesk.nic.in

5. Responsibility of Stakeholders

5.1 It is the duty of all the stakeholders (as mentioned in the Section 1.3 Scope of this Policy) to report any security incident to NIC-CERT, as soon as he/she comes to know of it.

5.2 All Users/Stakeholders, shall not withhold or destruct or falsify - any information or evidence or data, from NIC-CERT.

5.3 All Users/Stakeholders, shall co-operate with NIC-CERT and abide by the instructions, advisories, guidelines…etc., issued by NIC-CERT from time to time.

5.4 All Users/Stakeholders, shall co-ordinate with NIC-CERT Team for security incidents and provide necessary details, logs, evidences, other assistance….etc., to NIC-CERT Team as and when requested.

5.5 Users/Stakeholders shall carry out necessary changes in their devices, application, database, softwares, websites, services…etc, as per the advise of NIC-CERT, to mitigate against security threats. Upon taking necessary action, the Users/Stakeholders, shall report back to NIC-CERT with the action taken status.

5.5 All stakeholders shall consult or keep NIC-CERT keep informed of the activities undertaken for the investigation or mitigation of any security incident.

5.6 If Multiple Stakeholders are involved in the investigation or mitigation of a security incident or vulnerability, then all stakeholders shall consult and update NIC-CERT while undertaking the activity, so as to avoid any duplication or conflict of activities.

5.7 The Users/Stakeholders, who are involved in the investigation or mitigation of a Security incident, shall submit a detailed incident report (Ref.Annexure-II) on the incident, to NIC-CERT. The report shall be duly verified and sent through the respective HoDs/HoGs of each project/Division to NIC-CERT.

5.8 The Users/Stakeholders, shall maintain an updated Asset Register, with details of their Assets and Risk ratings. The list shall be periodically updated and shared with NIC-CERT, as and when any changes are done on the asset.

5.9 The Users/Stakeholders, shall patch their respective assets (hardware, software, application….etc) regularly and ensure that the latest patches are installed successfully on all their assets.

6.0 The Users/Stakeholders, shall ensure that appropriate Anti Virus solution (offered by NIC) is installed on all their system assets (like servers, PCs, laptops..etc) and it shall be kept updated with the latest Antivirus definitions/signatures.

6. Responsibility of NIC-CERT

6.1 NIC-CERT shall be the nodal agency for all Information Security Incidents happening in NIC's network or infrastructure or services.

6.2 NIC-CERT, shall act as a Single Point of Contact (SPOC), for the security incidents and shall co-ordinate between different stakeholders.

6.3 NIC-CERT, shall publish/circulate : security advisories, security guidelines, security best practices….etc., from time to time

6.4 NIC-CERT, shall maintain a knowledge base of Security Incidents, and details of their Investigation and Mitigation.

6.5 NIC-CERT, shall maintain a knowledge base of Security Advisories

6.6 Upon detection/knowledge, of any security incident or vulnerability, NIC-CERT shall notify the respective stakeholder for mitigation.

7. Information Security Incident Classification

Classification Level	Description	Example
Level 1	Breach of sensitive data or information, Unauthorized Access, Compromise of systems or data	Data Exfiltration, backdoor, unauthorized modification of data, content or configuration. Destroy or disrupt the devices, network or services of NIC, compromise of e-mail of sensitive officials.
Level 2	Network Compromise, DoS/DDoS,	UDP/SYN/Http Flooding, NTP Amplification, compromise of network/security devices,
Level 3	Malicious Program	Malware, APTs, Trojans, Virus
Level 4	NIC's Policy Violation	Sharing of passwords, Using NIC's e-mail for sending spams, Using NIC's network to launch malicious traffic against external networks..etc
Level 5	Reconnaissance Activity, Attempt to intrude	Unauthorized - Port scanning or scanning for vulnerabilities. Unauthorized Attempt to intrude into NIC's network/system/services.
Level 6	Others	This Level includes all other incidents which may not fit in the Levels 1 to 4.

7.1 Incident Severity: Impact-Urgency Matrix

I M P A C T	Multiple Ministries or States or Applications or Websites	High	High	Critical
	One or Two Ministries or States or Applications or Websites	Medium	High	Critical
	Single location or User or non-critical asset	Low	Medium	High
	URGENCY			

Note: All Incidents shall be classified based on Level and Severity. Any Security Incident from sensitive/VIP, Users like PMO, Cabinet Secretariat…etc, shall be treated as “Critical”.

8.0 Information Security Incident Response Ticket Flow