National Informatics Centre

SOP for Connecting a Machine to the Ministry Network

Owner: NIC- Cyber Security Division

CONFIDENTIALITY CLAUSE

This document is the property of National Informatics Centre (NIC). Every concept and piece of information within this document is the intellectual property of NIC. These documents are not for general distribution and are meant for use solely by the person/persons to whom it is specifically issued to. Copying or unauthorized distribution of these documents, in any form or means including electronic, mechanical, photocopying or otherwise is illegal.

CONTACT INFORMATION

For any question regarding this policy, please contact – NIC-CSG

Email:

Document Version Control

Document Version Control Note	
Name of the Document	SOP for Connecting a Machine to the Ministry Network
Document Version Number	1.0
Effective Date	
Approved By	
This Revision Supersedes	
Document Classification	Restricted
Distribution List	1.CIS Co-ordinator 2.CISO 3.DCISO 4.NIC-CSG
Access Level	Read Only

REVISION HISTORY

Version	Release Date	Prepared By	Reviewed By	Approved By	Description of changes made	Section of document Impacted
1.0					First Release	NA

Table of Contents

1. Abbreviations

Sr.No.	Abbreviations	Full Form
1.	CIS Coordinator	Cyber and Information Security Coordinators
2.	CISO	Chief Information Security Officer
3.	DCISO	Deputy Chief Information Security Officer
4.	MSP	Managed Service Provider
5.	NIC	National Informatics Centre
6.	NIC-CSG	NIC Cybersecurity Group
7.	SOP	Standard Operating Procedure

2. Definitions

Sr.No.	Expression	Definition
1.	Chief Information Security Officer	In relation to an Organisation, such officer as is designated by the Organisation as its Chief Information Security Officer, or if no officer is so designated, such officer as the NIC-CSG may specify
2.	Cyber and Information Security Coordinators	In relation to an Organisation, such officer as is designated by NIC-CSG for overseeing Deputy Chief Information Security Officers (DCISOs) and co-ordinate with the CISOs of the assigned Organisation for the responsibility of Information Security and Cybersecurity
3.	Cybersecurity team	Team comprised of Cybersecurity professionals, to be deployed by the MSP.
4.	Deputy Chief Information Security Officer	In relation to an Organisation, such officer who are designated by NIC-CSG and are assigned the responsibility of Information Security and Cybersecurity in an Organisation.
5.	ICT Inventory	A centralized record containing details of all ICT resource owned by the Organisation and it's enity, including their identification, location, status, and other relevant information.
6.	ICT resources/asset	In relation to an Organisation, the computer resources (including servers, virtual machines, containers and Endpoints), network components, peripheral devices (printers, scanners etc.),security devices and applications; (a) Owned by it or any of its agencies (b) Used by it but owned by NIC or any of its agencies, or by any other entity in respect of whose ICT Resources there is no work order in force, and which is under the control of such Organisation.
7.	ICT Team	In relation to an Organisation, the team of ICT professionals responsible for the management of its ICT resources
8.	Machine	Desktops, Laptops and any other media devices
9.	Managed Service Provider/MSP	The selected Bidder with whom NIC-CSG has entered into the contract for respective Organisation.
10.	NIC-CSG	The NIC Cybersecurity Group has been created to enhance the cybersecurity posture and to provide safe and secure cyber environment to Organisation
11.	Organisation	One or more entities to which NIC-CSG provides information and communication technology (ICT) services or support, including;

		(a) A ministry, department, secretariat or office of the Central Government specified in the First Schedule to the Government of India (Allocation of Business) Rules, 1961, and any other entity under the administrative purview of any such ministry, department, secretariat or office; (b) Secretariats or offices of Lok Sabha, Rajya Sabha, Supreme Court of India, Delhi High Court and other NIC supported Constitutional body or national level statutory body

3. Purpose

To outline the process required to securely connect a machine to the Ministry's network. This document ensures the best practices for securely and consistently connecting a machine in the Ministry's network.

4. Scope and Applicability

This procedure applies to all the employees, contractors, and third-party vendors who are responsible for connecting machines to the Ministry's network. This procedure applies to all the devices e.g., Desktops, Laptops and any other media devices which are required to be connected to the Ministry Network.

5. Pre-connection verification of the Machine

1.1 Document Machine Details

IT Department of the Ministry shall document the following details of the machine:

(i) Record the machine's make, model, serial number, and assigned IP address.

(ii) Note the machine's intended use and primary user.

(iii) Record the date and time of connection.

(iv) Ensure the machine's firewall is enabled and properly configured. Apply any necessary firewall rules specific to the machine's role.

(v) Check for Vulnerabilities by scanning the machine for any malware and other security threats.

(vi) Ensure the machine adheres to the Ministry's security policies e.g, Password policy, Software Update and Patch Management Policy, Access Control Policy, Backup and Recovery Policy etc.

(vii) Notify the network administrator and relevant stakeholders about the machine inclusion in the Ministry network.

1.2 Request and Reviews for connecting the Machine to the Network

(i) **Initiate Request for connecting to the Network**: A request form shall be filled out mentioning the following information and submitted to the Ministry for review and approval.

- Purpose for connecting the machine to the network.
- Requestor Name, Department/Organisation and Contact information.
- Device Type (e.g., desktop, laptop, server, IoT device)
- Make and Model
- Serial Number
- MAC Address
- Operating System
- Installed Software
- Required Network Resources (e.g., specific servers, databases)
- Details of Installed Security Software (e.g., Antivirus, Firewalls etc.)
- Any other relevant information or special requirements.

(ii) **Submission of Request Form:** Submit the completed Network Connection Request Form to the IT department of the Ministry through the designated method (e.g., email, ticketing system, online portal).

(iii) **Acknowledgement of the Request Form**: The IT department shall acknowledge the receipt of the request and provides a reference number for tracking purposes.

(iv) **Review by IT Department:** The IT department shall review the request for completeness and accuracy. If additional information is needed, the requestor is contacted to provide the required details. IT department shall confirm that the request aligns with the Ministry's policies and network capacity

6. Approval by DCISO for connecting the Machine to the Network

(i) DCISO shall verify and ensure that the machine connection is justified for Ministry/Department needs.

(ii) They shall also confirm that the device supports the organization's objectives and operations.

(iii) Verify that the machine's connectivity is necessary.

(iv) Confirm that the machine has been scanned for vulnerabilities and that any identified issues have been addressed.

(v) Check that the machine complies with the Ministry's IT and security policies.

(vi) Ensure adherence to relevant regulatory and legal requirements (e.g., data protection laws).

(vii) DCISO shall provide final approval only after confirming all criteria are satisfactorily met.

7. Reference

Sr. No.	Document name	Attachment
1.		