



फा.सं. 5-2/2022-ई.सी./4582-4586

राष्ट्रीय शैक्षिक अनुसंधान एवं प्रशिक्षण परिषद
श्री अरविंद मार्ग, नई दिल्ली -110016
(स्थापना समन्वय अनुभाग)

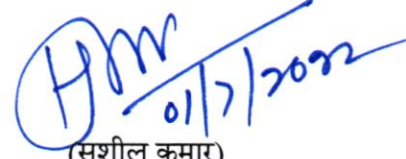
दिनांक : 01.07.2022

परिपत्र

**विषय : [Secy-GoI] Cyber Security Guidelines for Government Employees- issued
For wide circulation and strict compliance – reg.**

उपरोक्त विषय पर Deputy Director General to the Government of India, National Informatics Centre, Ministry of Electronics & Information Technology से प्राप्त ई-मेल दिनांक 14.06.2022 की प्रतिलिपि सूचना एवं अनुपालन हेतु ई-ऑफिस (KMS) एवं ई-मेल द्वारा परिचालित की जा रही है।

यह सक्षम अधिकारी के अनुमोदन से जारी किया जा रहा है।


(सुशील कुमार)
अवर सचिव

संलग्नक: उपरोक्तनुसार

1. संयुक्त निदेशक, सी.आई.ई.टी.।
2. संयुक्त निदेशक, पी.एस.एस.सी.आई.वी.ई., श्यामला हिल भोपाल।
3. डीन (अ)/ डीन (सी)/ डीन (आर) एन.सी.ई.आर.टी.।
4. एन.आई.ई. के सभी विभागों के अध्यक्ष।
5. प्राचार्य, क्षेत्रीय शिक्षा संस्थान, अजमेर/भोपाल/भुवनेश्वर/मैसूर/शिलांग।
6. मुख्य लेखाधिकारी, एन.सी.ई.आर.टी.।
7. सभी उपसचिव/अवर सचिव, एन.सी.ई.आर.टी.।
8. प्रशासनिक अधिकारी, प्रकाशन विभाग, एन.सी.ई.आर.टी.।
9. व्यावसायिक प्रबन्धक, राज्यों में आर.पी.डी.सी. (गुवाहाटी, अहमदाबाद, बेंगलुरु, कोलकाता)।
10. एन.आई.ई. के सभी अनुभाग/प्रकोष्ठ।
11. निदेशक, एन.सी.ई.आर.टी. के निजी सचिव।
12. संयुक्त निदेशक, एन.सी.ई.आर.टी. के निजी सचिव।
13. सचिव, एन.सी.ई.आर.टी. के निजी सचिव।



Establishment Coordination <ecsection7@gmail.com>

Fwd: [Secy-go] Cyber Security Guidelines for Government Employees - issued For wide circulation and strict compliance

1 message

Sridhar Srivastava <jd.ncert@nic.in>
To: ecsection7 <ecsection7@gmail.com>

Tue, Jun 14, 2022 at 10:53 AM

महोदय,

मुझे अनुगामी ईमेल को संलग्नकों सहित अवलोकन और आवश्यक कार्रवाई हेतु अग्रेषित करने का निर्देश हुआ है।

सधन्यवाद !

संयुक्त निदेशक कार्यालय
रा. शै. अनु. और प्र. प.
श्री अरविन्द मार्ग
नई दिल्ली-110 016
दूरभाष : 011-26510105

From: "Dinesh Prasad Saklani" <director.ncert@nic.in>
To: "Amarendra P Behera" <jdciet.ncert@nic.in>, "Pratyusa Kumar Mandal" <secy.ncert@nic.in>
Cc: "Sridhar Srivastava" <jd.ncert@nic.in>
Sent: Tuesday, June 14, 2022 9:49:04 AM
Subject: Fwd: [Secy-go] Cyber Security Guidelines for Government Employees - issued For wide circulation and strict compliance

From: "Vipin Kumar" <jscord-education@nic.in>
To: "L Sweety Changsan" <lischangsan@nic.in>, "MANEESH GARG IAS" <maneesh.garg@nic.in>, "Ms Geetu Joshi" <g.sjoshi@nic.in>, "R.C. Meena" <r.cmeena@nic.in>, "R.C. Meena" <r.cmeena@gov.in>, "Venkatramana R" <v.hegde@nic.in>, "Santosh Kumar Yadav" <yadavsk.up@nic.in>, "nbb admin" <nbb.admin@gmail.com>, "Chairperson CBSE" <chmn-cbse@nic.in>, directorctsadelhi@gmail.com, cm@nios.ac.in, cp@ncte-india.org, "kvs commissioner" <kvs.commissioner@gmail.com>, "Vinayak Garg" <commissioner.nvs@gov.in>, "Nidhi Panday" <commissioner-kvs@gov.in>, ms@ncte-india.org, commissioner.nvs@yahoo.com, "Dinesh Prasad Saklani" <director.ncert@nic.in>, "Ashwani Kumar" <kumar.aswani@nic.in>, "Saba Akhtar" <saba@nic.in>
Sent: Monday, June 13, 2022 8:14:16 PM
Subject: Fwd: [Secy-go] Cyber Security Guidelines for Government Employees - issued For wide circulation and strict compliance

From: "Ms Anita Karwal" <secy.sel@nic.in>
To: "Vipin Kumar" <jscord-mhrd@gov.in>
Sent: Monday, June 13, 2022 9:35:25 AM
Subject: Fwd: [Secy-go] Cyber Security Guidelines for Government Employees - issued For wide circulation and strict compliance

24 No. 359/22
15/6/22

Sanjay Dnyu
15/6/2022

From: "Seema Khanna" <seema@gov.in>
To: chiefsecretaries@ismgr.nic.in, secy-goi@ismgr.nic.in
Cc: "Director General NIC" <dg@nic.in>, "Secretary MeitY" <secretary@mit.gov.in>, "Dr(Mr) Rajendra Kumar" <as@meity.gov.in>
Sent: Monday, June 13, 2022 9:23:00 AM
Subject: [Secy-goi] Cyber Security Guidelines for Government Employees - issued For wide circulation and strict compliance

Dear Sir/Madam

Please find enclosed the "Cyber Security Guidelines for Government Employees".

The guideline specifies the "do's and don'ts" with respect to cyber security and ensuring proper cyber security hygiene in the government offices.

It is requested that these guidelines maybe circulated amongst all officers in your State/Ministry/Department for compliance by all, including the outsourced/contractual manpower.

A workshop is also being planned for the Department Heads and CISOs for sensitizing them on this guideline. The schedule for the workshop and its related details shall be communicated shortly.

This mail is being sent as per the directions of Secretary MeitY.

regards

Seema Khanna
Deputy Director General
National Informatics Centre
Ministry of Electronics & Information Technology
Government of India



Disclaimer:

This e-mail and its attachments may contain official Indian Government information. If you are not the intended recipient, please notify the sender immediately and delete this e-mail. Any dissemination or use of this information by a person other than the intended recipient is unauthorized. The responsibility lies with the recipient to check this email and any attachment for the presence of viruses.

Secy-goi mailing list -- secy-goi@ismgr.nic.in
To unsubscribe send an email to secy-goi-leave@ismgr.nic.in



 **Cyber_Security_Guidelines_for_Govt_Employees-Final_Release.pdf**
388K



Establishment Coordination <ecsection7@gmail.com>

Fwd: Cyber Security Guidelines for Government Employees - issued For wide circulation and strict compliance

1 message

Sridhar Srivastava <jd.ncert@nic.in>
To: ecsection7 <ecsection7@gmail.com>

Tue, Jun 14, 2022 at 10:52 AM

महोदय,

मुझे अनुगामी ईमेल को संलग्नकों सहित अवलोकन और आवश्यक कार्रवाई हेतु अग्रेषित करने का निर्देश हुआ है।

सधन्यवाद !

संयुक्त निदेशक कार्यालय
रा. शै. अनु. और प्र. प.
श्री अरविन्द मार्ग
नई दिल्ली-110 016
दूरभाष : 011-26510105

From: "Dr. Seema Khanna" <seema@gov.in>
To: "jd ncert" <jd.ncert@nic.in>
Sent: Monday, June 13, 2022 9:00:38 PM
Subject: Cyber Security Guidelines for Government Employees - issued For wide circulation and strict compliance

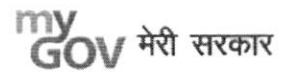
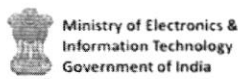
Dear Sir/Madam

Please find the link to the "Cyber Security Guidelines for Government Employees".

The guideline specifies the "do's and don'ts" with respect to cyber security and ensuring proper cyber security hygiene in the government offices including the contractual/outsourced manpower. It is requested that these guidelines maybe circulated amongst all officers in your State/Ministry/Department for compliance by all, including the outsourced/contractual manpower.

This mail is being sent on the directions of Director General, National Informatics Centre .

Regards,
Seema Khanna
Deputy Director General
National Informatics Centre
Ministry of Electronics & Information Technology
Government of India



Cyber Security Guidelines for Government Employees



MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY



A-Block, CGO Complex

New Delhi – 110003

Website: <https://www.nic.in/>

DOCUMENT CONTROL

DOCUMENT NAME: Cyber Security Guidelines for Government Employees

DOCUMENT ID REFERENCE: CGGE

AUTHORIZATION:

S.No	Name	Designation	Role
1	Shri Alkesh Kumar Sharma	Secretary, MeitY	Approving Authority
2	Dr Rajendra Kumar	AS, MeitY	Reviewer
2	Shri Rajesh Gera	DG, NIC	Reviewer
3	Dr. Sanjay Bahl	DG, CERT-In	Reviewer
4	Shri R.S. Mani	DDG, NIC	Reviewer
5	Shri C.J. Antony	DDG, NIC	Reviewer
6	Dr. Seema Khanna	DDG, NIC	Reviewer
7	Shri S.S. Sharma	Scientist-F, CERT-In	Reviewer
8	Shri Hari Haran	SSA, NIC	Author

SECURITY CLASSIFICATION: Restricted

VERSION HISTORY:

Issue Date	Effective Date	Description
1.1	7-Jun-2022	Draft- Added Section-5, Cyber Security Resources
1.2	8-Jun-2022	Draft – Added inputs from CERT-In and included DNS Server IPv4 and IPv6 IP addresses.
1.3	10-Jun-2022	Final Release

DISTRIBUTION LIST:

The following persons hold copies of the documents; all amendments and updates to the document must be distributed to the distribution list.

S.No.	Name	Location	Document type
1	Government Ministries and Departments	Across India	Soft copy

CONFIDENTIAL:

This document contains restricted information pertaining to the National Informatics Centre. The access level for the document is specified above. The addressee should honor this access right by preventing intentional or accidental access outside the access scope.

DISCLAIMER:

This document is solely for the information of the government employees and outsourced/contractual resources and it should not be used, circulated, quoted or otherwise referred to for any other purpose, nor included or referred to in whole or in part in any document without our prior written consent of NIC/MeitY.

TABLE OF CONTENTS

1	Introduction.....	5
2	Cyber Security Do's	5
3	Cyber Security Don'ts.....	7
4	Cyber Security Resources.....	9
5	Compliance	10

1 INTRODUCTION

Information and communication technologies (ICT) have become ubiquitous amongst government ministries and departments across the country. The increasing adoption and use of ICT has increased the attack surface and threat perception to government, due to lack of proper cyber security practices followed on the ground. In order to sensitize the government employees and contractual/outsourced resources and build awareness amongst them on what to do and what not to do from a cyber security perspective, these guidelines have been compiled. By following uniform cyber security guidelines in government offices across the country, the security posture of the government can be improved.

2 CYBER SECURITY DO'S

1. Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters.
2. Change your passwords at least once in 45 days.
3. Use multi-factor authentication, wherever available.
4. Save your data and files on the secondary drive (ex: d:\).
5. Maintain an offline backup of your critical data.
6. Keep your Operating System and BIOS firmware updated with the latest updates/patches.
7. Install enterprise antivirus client offered by the government on your official desktops/laptops. Ensure that the antivirus client is updated with the latest virus definitions, signatures and patches.
8. Configure NIC's DNS Server IP (IPv4: 1.10.10.10 / IPv6: 2409::1) in your system's DNS Settings.

9. Configure NIC's NTP Service (samay1.nic.in, samay2.nic.in) in your system's NTP Settings for time synchronization.
10. Use authorized and licensed software only.
11. Ensure that proper security hardening is done on the systems.
12. When you leave your desk temporarily, always lock/log-off from your computer session.
13. When you leave office, ensure that your computer and printers are properly shutdown.
14. Keep your printer's software updated with the latest updates/patches.
15. Setup unique passcodes for shared printers.
16. Use a Hardware Virtual Private Network (VPN) Token for connecting privately to any IT assets located in the Data Centres.
17. Keep the GPS, bluetooth, NFC and other sensors disabled on your computers and mobile phones. They maybe enabled only when required.
18. Download Apps from official app stores of google (for android) and apple (for iOS).
19. Before downloading an App, check the popularity of the app and read the user reviews. Observe caution before downloading any app which has a bad reputation or less user base, etc.
20. Use a Standard User (non-administrator) account for accessing your computer/laptops for regular work.
21. While sending any important information or document over electronic medium, kindly encrypt the data before transmission. You can use a licensed

encryption software or an Open PGP based encryption or add the files to a compressed zip and protect the zip with a password. The password for opening the protected files should be shared with the recipient through an alternative communication medium like SMS, Sandes, etc.

22. Observe caution while opening any shortened uniform resource locator (URLs) (ex: tinyurl.com/ab534/). Many malwares and phishing sites abuse URL shortener services.
23. Observe caution while opening any links shared through SMS or social media, etc., where the links are preceded by exciting offers/discounts, etc., or may claim to provide details about any current affairs. Such links may lead to a phishing/malware webpage, which could compromise your device.
24. Report suspicious emails or any security incident to incident@cert-in.org.in and incident@nic-cert.nic.in.
25. Adhere to the security advisories published by NIC-CERT (<https://nic-cert.nic.in/advisories.jsp>) and CERT-In (<https://www.cert-in.org.in>).

3 CYBER SECURITY DON'TS

1. Don't use the same password in multiple services/websites/apps.
2. Don't save your passwords in the browser or in any unprotected documents.
3. Don't write down any passwords, IP addresses, network diagrams or other sensitive information on any unsecured material (ex: sticky/post-it notes, plain paper pinned or posted on your table, etc.)

4. Don't save your data and files on the system drive (Ex: c:\ or root).
5. Don't upload or save any internal/restricted/confidential government data or files on any non-government cloud service (ex: google drive, dropbox, etc.).
6. Don't use obsolete or unsupported Operating Systems.
7. Don't use any 3rd party DNS Service or NTP Service.
8. Don't use any 3rd party anonymization services (ex: Nord VPN, Express VPN, Tor, Proxies, etc.).
9. Don't use any 3rd party toolbars (ex: download manager, weather tool bar, askme tool bar, etc.) in your internet browser.
10. Don't install or use any pirated software (ex: cracks, keygen, etc.).
11. Don't open any links or attachments contained in the emails sent by any unknown sender.
12. Don't share system passwords or printer passcode or Wi-Fi passwords with any unauthorized persons.
13. Don't allow internet access to the printer.
14. Don't allow printer to store its print history.
15. Don't disclose any sensitive details on social media or 3rd party messaging apps.
16. Don't plug-in any unauthorized external devices, including USB drives shared by any unknown person
17. Don't use any unauthorized remote administration tools (ex: Teamviewer, Ammy admin, anydesk, etc.)

18. Don't use any unauthorized 3rd party video conferencing or collaboration tools for conducting sensitive internal meetings and discussions.
19. Don't use any external email services for official communication.
20. Don't jailbreak or root your mobile phone.
21. Don't use administrator account or any other account with administrative privilege for your regular work.
22. Don't use any external mobile App based scanner services (ex: Camscanner) for scanning internal government documents.
23. Don't use any external websites or cloud-based services for converting/compressing a government document (ex: word to pdf or file size compression)
24. Don't share any sensitive information with any unauthorized or unknown person over telephone or through any other medium.

4 CYBER SECURITY RESOURCES

The following resources may be referred for more details regarding the cyber security related notifications/information published by Government of India:

S.No	Resource URL	Description
1	https://www.meity.gov.in/cyber-security-division	Laws, Policies & Guidelines
2	https://www.cert-in.org.in	Security Advisories, Guidelines & Alerts
3	https://nic-cert.nic.in	Security Advisories, Guidelines & Alerts
4	https://www.csk.gov.in	Security Tools & Best Practices
5	https://infosecawareness.in/	Security Awareness Materials
6	http://cybercrime.gov.in	Report Cyber Crime, Cyber Safety Tips

5 COMPLIANCE

All government employees, including temporary, contractual/outsourced resources are required to strictly adhere to the guidelines mentioned in this document. Any non-compliance may be acted upon by the respective CISOs/Department heads.