पत्रांक–07–सू0प्रा0–17 / 2023 335

बिहार सरकार

सूचना प्रावैधिकी विभाग

प्रेषक,

संतोष कुमार मल्ल,
सरकार के प्रधान सचिव।

सेवा में,

अपर मुख्य सचिव / प्रधान सचिव / सचिव
सभी विभाग, बिहार, पटना।

पटना, दिनांक 09.02.2023

विषय :– सरकारी कार्यालयों में कार्यरत कर्मचारियों के लिए Cyber Security दिशा–निर्देश के संबंध में।

महाशय,

आप अवगत हैं कि e-Governence को प्रभावी ढंग से लागू करने के क्रम में Information and Communication Technologies (ICT) देश के सभी सरकारी मंत्रालयों एवं विभागों के बीच सर्वव्यापी हो गयी है। बिहार सरकार के विभिन्न विभाग भी ICT का इष्टतम उपयोग कर रहे हैं, लेकिन उचित Cyber Security Practice के अभाव में सरकारी IT Infrastructure पर Cyber हमले व Data Theft के खतरे की संभावना बनी रहती है।

इस संबंध में सरकारी कर्मचारियों और संविदाकर्मियों / आउटसोर्स मानव संसाधनों को Cyber Security के प्रति सुग्राही बनाने एवं साईबर सुरक्षा के दृष्टिकोण से क्या करें और क्या नहीं करें (Do's & Don'ts) की जानकारी देने के लिए भारत सरकार के द्वारा Cyber Security Guidelines जारी किया गया है, जिसकी प्रति पत्र के साथ संलग्न है। राज्य के सभी कार्यालयों में उक्त दिशा–निर्देशों का पालन करके Cyber Security की स्थिति में सुधार लाया जा सकता है।

अतः अनुरोध है कि अपने विभाग एवं अधीनस्थ बोर्ड / निगम / संस्थान में सरकारी कर्मचारियों और संविदाकर्मियों / आउटसोर्स मानव संसाधनों के बीच उक्त Cyber Security दिशा–निर्देशों का व्यापक प्रचार प्रसार एवं अनुपालन सुनिश्चित कराया जाय।

विश्वासभाजन,

संतोष 8/2/23

(संतोष कुमार मल्ल)
सरकार के प्रधान सचिव।

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

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.