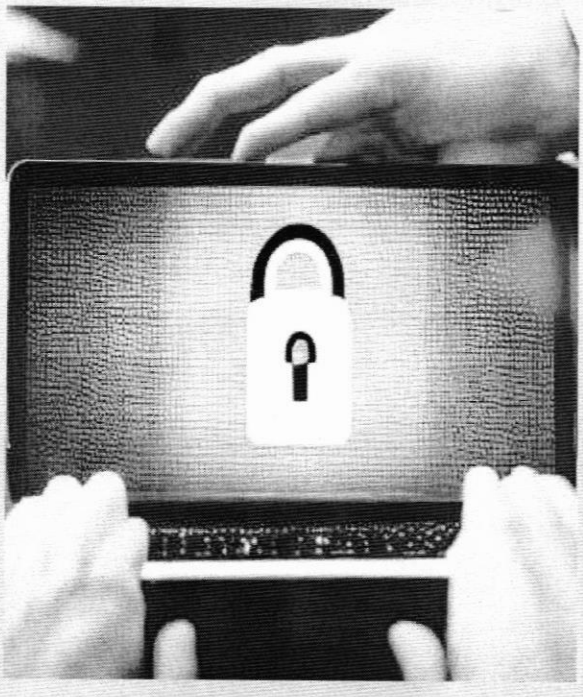
Cybersecurity Appropriate Behaviour for Government Employees of Assam

Document Version V1



Information Technology
DepartmentGovernment of Assam

Contents

A. INTRODUCTION

Cybersecurity appropriate behaviour is of utmost importance for Government employees because they handle sensitive information that, if accessed by unauthorized parties, can pose significant threats to national security. Government employees are entrusted with critical information, such as classified data, personal information of citizens, and other confidential records that require stringent security measures. A cybersecurity appropriate behaviour list is required for Government employees to ensure that they follow best practices to protect sensitive information from cyber threats. The list provides guidelines, protocols, and compliance requirements to follow, reduces the risk of insider threats, and promotes a culture of security within Government agencies.

In the View of the above, we have prepared a guideline in the form of "Do's and Don'ts" for appropriate cyber behaviour of Government employees of Assam to develop cyber safe resilience ecosystem in the Government of Assam.

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.

B. COMMON CYBER SECURITY: DO'S AND DON'TS

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 3 months
3. Use multi-factor authentication, wherever available.
4. Save your important data and files on the secondary drive in the system
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 DNS Server IP and NTP Service as recommended by System Administrator / NIC.
9. Use authorized and licensed software only.
10. Ensure that proper security hardening is done on the systems.
11. When you leave your desk temporarily, always lock/log-off from your computer session.
12. When you leave office, ensure that your computer and printers are properly shutdown.
13. Keep your printer's software updated with the latest updates/patches.
14. Setup unique passcodes for shared printers.
15. Use Virtual Private Network (VPN) for connecting remotely to any IT assets located in the Data Centres / office resources from home / public network.
16. Keep the GPS, bluetooth, NFC and other sensors disabled on your computers and mobile phones. They maybe enabled only when required.