ASSAM ELECTRICITY GRID CORPORATION LIMITED
OFFICE OF THE MANAGING DIRECTOR
Regd. Office:(FIRST FLOOR), BIJULEE BHAWAN, PALTANBAZAR; GUWAHATI - 781001
CIN: U40101AS2003SGC007238 GSTIN: 18AAFCA4973J9Z3
PHONE: 0361-2739520 Web: www.aegcl.co.in

File No. AEGCL/MD/TECH-903/Cyber Security/2020/ 31 **Date: 27/4/21.**

OFFICE ORDER

This is for the information of all the concerned that AEGCL has prepared a "Cyber Security Guidelines" for the IT equipment like Desktop PC/Laptop/SCADA used in the offices of AEGCL including the HQ.

All the officials are requested to follow the Cyber security Guidelines at their respective offices while using the IT equipment. The process of properly following the guidelines will be acting as the protective shield against the cyber threats and vulnerabilities.

The guidelines will be updated on time-to-time basis as envisioned by the IT Team. Further suggestions for improvement of the guidelines are welcome and may be processed as and when required.

This is for your information and necessary action.

Chief General Manager (T&C and Communication)
AEGCL, Bijulee Bhawan

Memo No.: File No. AEGCL/MD/TECH-903/Cyber Security/2020/ 31(a) **Date: 27/4/21**

Copy to:

1. PS to MD, AEGCL, Bijulee Bhawan, Paltanbazar, Guwahati-01 for kind appraisal.
2. All Chief General Managers, Bijulee Bhawan, AEGCL
3. All General Managers, field offices of AEGCL
4. All Deputy General Managers, field offices of AEGCL
5. All Assistant General Managers, field offices of AEGCL
6. All Deputy Managers, field offices of AEGCL
7. All Assistant Managers, field offices of AEGCL
8. AAO/DAO/AO
9. All REs of GSS
10. All the concerned Staff
11. Office Copy

27/04/2021

Chief General Manager (T&C and Communication)
AEGCL, Bijulee Bhawan

Cyber Security Guidelines

ASSAM ELECTRICITY GRID CORPORATION LTD.

Backbone of Assam Power Network

অসম বিদ্যুৎ সংবহন নিগম লিমিটেড

অসমৰ বিদ্যুৎ ক্ষেত্ৰৰ মেৰুদণ্ড

Prepared By

IT Team, AEGCL

1. Information Sharing and Analysis Center (ISAC – Power)

Cyber security of Critical Infrastructure is a growing concern among business and Governments worldwide. Information Sharing and Analysis Centre (ISAC-Power) is a central coordinating agency to share and analyze various cyber security incidents in the Power Sector. It is the common platform for the five Sectoral CERTs under Ministry of Power.

The Government of India, through Information Technology Act-2000 laid the foundation of CERT-In, an organization dedicated to the cause of Cyber Security standards, compliances, Incident Response and Guidance. The Government of India after reviewing the needs of cyber security in Critical Infrastructure sector, created dedicated Sectoral CERTs mentioned below:

Sectoral CERT	Nodal Organization
CERT – Thermal	NTPC
CERT – Hydro	NHPC
CERT – Transmission	**POWERGRID**
CERT – Distribution	DP&T Division, CEA
CERT – Grid Operation	NLDC

2. National Critical Information Infrastructure Protection Centre (NCIIPC)

National Critical Information Infrastructure Protection Centre (NCIIPC) is an organization of the Government of India created under Sec 70A of the Information Technology Act, 2000 (amended 2008), through a gazette notification on 16th Jan 2014 based in New Delhi, India. It is designated as the National Nodal Agency in respect of Critical Information Infrastructure Protection.

Vision

To facilitate safe, secure and resilient Information Infrastructure for Critical Sectors of the Nation.

Mission

To take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or distraction through coherent coordination, synergy and raising information security awareness among all stakeholders.

Functions and Duties

- National nodal agency for all measures to protect nation's critical information infrastructure.
- Protect and deliver advice that aims to reduce the vulnerabilities of critical information infrastructure, against cyber terrorism, cyber warfare and other threats.
- Identification of all critical information infrastructure elements for approval by the appropriate Government for notifying the same.
- Coordinate, share, monitor, collect, analyse and forecast, national level threat to CII for policy guidance, expertise sharing and situational awareness for early warning or alerts. The basic responsibility for protecting CII system shall lie with the agency running that CII.
- Developing or organising training and awareness programs as also nurturing and development of audit and certification agencies for protection of Critical Information Infrastructure.
- Issuing guidelines, advisories and vulnerability or audit notes etc. relating to protection of critical information infrastructure and practices, procedures, prevention and response in consultation with the stake holders, in close coordination with Indian Computer Emergency Response Team (CERT) and other organisations working in the field or related fields.
- Exchanging cyber incidents and other information relating to attacks and vulnerabilities with Indian Computer Emergency Response Team (CERT-In) and other concerned organisations in the field.
- In the event of any threat to critical information infrastructure the National Critical Information Infrastructure Protection Centre may call for information and give directions to the critical sectors or persons serving or having a critical impact on Critical Information Infrastructure.

3. Who is CERT- In

CERT-In (the Indian Computer Emergency Response Team) is a government-mandated information technology (IT) security organization. It strengthens security-related defence of the Indian Internet domain. CERT-In was created by the Indian Department of Information Technology in 2004 and operates under the auspices of that department. According to the provisions of the Information Technology Amendment Act 2008The purpose of CERT-In is to respond to computer security incidents, report on vulnerabilities and promote effective IT security practices throughout the country.

Vision

Proactive Contribution in Securing India's cyber space

Mission

To enhance the security of India's Communications and Information Infrastructure through proactive action and effective collaboration.

Objectives

- Preventing cyber-attacks against the country’s cyber space
- Responding to cyber-attacks and minimizing damage and recovery time reducing “National vulnerability to Cyber-attacks”.
- Enhancing security awareness among citizens.

It is suggested to follow a common Cyber Security Policy / Guideline as a countermeasure to vulnerability to Cyber Attacks.

4. Why Cyber Security policy so essential?

A written policy serves as a formal guide to all cybersecurity measures used. It allows the security specialists and employees to be on the same page and gives a way to enforce rules that protect the data. However, the workflow of each department can be unique and can easily be disrupted by needless cybersecurity measures. While a centralized security policy can be beneficial as a basic guideline for the whole company, and it must ensure that the workflows won’t be compromised in the name of security.

In this context, AEGCL has prepared Cyber Security guidelines for the office Desktop PC/ Laptop that is needed to be followed with at most priority at all the offices of AEGCL.

5. Guidelines for IT euipments (Desktop/Laptop):

1. Backing up data is one of the information security best practices that has gained increased relevance in recent years, so, maintain regular backups of data to avoid the risk of data loss.

2. Install and maintain updated anti-virus and anti-spyware software at desktop / Laptop level.

3. Scan computer system with updated anti-virus for possible infections and disinfect the same. It is advised to take the complete backup of affected system prior disinfecting the same with the tools provided.

   One can visit the website of "Cyber Swachhta Kendra" (CSK) to download the "Free Bot Removal Tool" and disinfect systems.
   Website: https://www.CSK.gov.in

4. Install and maintain personal Desktop Firewall.

5. Check for the suspicious network activities of infected computer system mentioned in list and disinfect the same if found.

6. Use only genuine software and regularly update the patches.

7. Enable Windows Defender Application Guard with designated the trusted sites as whitelisted, so that rest all sites will be open in container to block the access to memory, local storage, other installed applications or any other resources of interest to the attacker.

8. Systems having an antivirus and a malware protection program on it and making sure they are always up to date. Systems and installed applications being fully patched and updated.

9. Scan for and remove suspicious e-mail attachments. Ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header). Block attachments of file types: [exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf].

10. Ensure to Scan all software downloaded from the Internet prior to execution/installation.

11. Do not browse un-trusted websites or follow un-trusted links and exercise caution while click on the link provided in any unsolicited emails.

12. Maintain logs of system/network and preserve the same to enable appropriate incident response/forensics.

13. Majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, can establish an essential pillar of defence.

14. Monitor Connection attempts towards the malicious IP/Domains. It may include compromised IP/Domains resources as well. Blocking the IP/Domains is solely the recipient responsibility after diligently verifying them without impacting the operations.

15. Disable unnecessary ports, protocols & services on workstations and servers. Monitor common ports and protocols for malicious Activity.

16. A compromised printer, for instance, can allow malicious actors to view all documents that are being printed or scanned. Ensure proper authentication to allow only trusted connections to endpoints is mandatory.

17. It always pays to mention the importance of thoughtful passwords and secure password handling. Password management is a key part of cyber security, passwords need to be long, complex and fully unique.

18. Passwords should be changed after a regular interval of time.

19. A great way to protect the sensitive data from breaches via third-party access is to monitor third-party actions. The scope of access of third-party users should be limited and exactly who is connected must be known.

6. **Guidelines for SaaS System/ SCADA:**

In addition to the Cyber Security guidelines for office use Desktop/Laptop, mentioned above in the point 5, the SCADA system must take care of the following:

1. Connectivity of SaaS systems with Internet should be restricted.
2. Authentication of the company persons coming for maintenance activities must be done.
3. Log details of all the visits should be maintained properly.
4. Unauthorized use of removable devices to the SCADA systems must be prohibited.
5. Entry of any unauthorized person to the SaaS system room should be prohibited.
6. Regular back up of data in the SaaS/SCADA systems must be taken.

*The “**Cyber Security Guidelines**” is prepared for the daily used Desktop/Laptop at the AEGCL offices and also for the SaaS system/SCADA. All the AEGCL officials must follow the Cyber Security guidelines as the security measures towards the probable vulnerabilities which may lead to Cyber-attack.*

The guidelines will be updated on time-to-time basis as envisioned by the Cyber security Team. Further suggestions for improvement of the guidelines will be highly appreciated.