பாரதியார் பல்கலைக்கழகம்

BHARATHIAR UNIVERSITY

COIMBATORE – 641 046, TAMILNADU, INDIA

State University	Accredited with "A++" Grade by NAAC	Ranked 26th among Indian Universities by MHRD-NIRF

No.C6/H.E./Cyber Security / 10762 -1/2025 Date : 07.07.2025

CIRCULAR

I am to inform that, the Additional Chief Secretary to Government, Information Technology & Digital Service Department, Secretariat, Chennai has directed to train Government employees in Cyber Security and prepare a set of Do's and Don'ts (Annexure enclosed) for them to minimise security risks in the workplace.

Hence, all the Heads of the Departments/Officers are requested to circulate it among the Faculty Members/Staffs / Students.

REGISTRAR i/c 7/7/25

Encl:

Cyber Security Guidelines: Do's and Don'ts

To

All the Heads of the Departments / Officers,
Bharathiar University.

BHARATHIAR UNIVERSITY ★ REGISTRAR ★ CBE-46

Copy to : 1. The P.S. to VC's Convenor Committee, B.U.
2. The P.A. to Registrar, B.U.
3. The University Engineer i/c, B.U.
4. The PRO i/c, B.U.
5. The Co-ordinator,
Centre for Internet and Website Services, B.U.

Annexure

Cyber Security Guidelines: Do's and Don'ts

Do's

1. **Use Strong Passwords:**

   - Complex passwords using a combination of uppercase letters, lowercase letters, numbers, and special characters. Aim for at least 8 characters.
   - Use unique passwords for different accounts, especially work related accounts.

2. **Enable 2-Factor Authentication:**

   - Many platforms now allow you to enable 2-factor authentication to keep your accounts more secure. It's another layer of protection that helps verify that it's you who is accessing your account and not someone who's unauthorized.
   - Enable this security feature when you can.

3. **Regularly Update Passwords:**

   - Change passwords every month and immediately if you suspect any account compromise.

4. **Keep Software up-to-date:**

   - Regularly update all software, including operating systems, applications, and antivirus programs. Many updates contain critical security patches.
   - Always update to the latest version of your software to protect yourself from new or existing security vulnerabilities.

5. **Keep hardware up-to-date:**

   - Department ensure the authorised life cycle of the hardware and software.

6. **Use anti-virus and anti-malware:**

   - If you're connected to the web, it's impossible to have complete and total protection from malware. However, you can significantly reduce your vulnerability by ensuring you have an anti-virus and at least one anti-malware software installed on your computers.

7. Remove adware from your machines:

   - Adware collects information about you to serve you more targeted ads. It's best to rid your computer of all forms of adware to maintain your privacy. Use AdwCleaner to clean adware and unwanted programs from your computer.

8. **Scan external storage devices for viruses:**

   - External storage devices are just as prone to malware as internal storage devices. If you connect an infected external device to your computer, the malware can spread. Always scan external devices for malware before accessing them.

9. **Train employees:**

   - The key to making Cyber Security work is to make sure your employees well trained, in sync, and consistently exercising security practices. Sometimes, one mistake from an improperly trained employee can cause an entire security system to crumble.

10. **Check links before you click:**

    - Links can easily be disguised as something they're not so it's best to double check before you click on a hyperlink. On most browsers, you can see the target URL by hovering over the link. Do this to check links before you click on them.

11. **Use a VPN to privatize your connections:**

    - Connect only to secure, password-protected Wi-Fi networks. Use a VPN if you need to access work resources from a public Wi-Fi network.

12. **Disable Bluetooth when you don't need it:**

    - Devices can be hacked via Bluetooth and subsequently your private information can be stolen. If there's no reason to have your Bluetooth on, turn it off!

13. **Lock Devices When Not in Use:**

    - Lock your computer, phone, or tablet when you step away from your desk, even if it's only for a short time.

14. **Report Suspicious Activity:**

    - Immediately report any suspicious emails, messages, or activity to the IT/TN-CERT security team. Early reporting can help prevent security incidents.

15. Secure Personal Devices:

- If you're allowed to use personal devices for work, ensure they have antivirus protection, are updated regularly, and are password protected.

16. **Back up Data Regularly:**

- Follow your organization's backup policy and store copies of essential data as per guidelines. This helps recover data in case of accidental loss or ransomware.

17. **Follow Organization Policies:**

- Adhere to your organization's Cyber Security policies, such as data handling, email usage, and internet browsing guidelines.

Dont's

1. **Don't Share Passwords:**

- Never share your work-related passwords with colleagues or anyone else. Avoid writing passwords down or storing them in unsecure places.

2. **Don't Click on Suspicious Links or Attachments:**

- Be cautious with emails from unknown senders or unexpected attachments, even if they appear to come from a known contact. These could be phishing attempts.

3. **Don't Ignore Security Warnings:**

- Take security warnings seriously. If your antivirus or security software flags something, report it to IT team, if you're unsure how to handle it.

4. **Don't Leave Sensitive Information Unattended:**

- Avoid leaving printed documents, USB drives, or devices with sensitive information in unsecured places. Store them securely when not in use.

5. **Don't Install Unauthorized Software:**

- Only use IT team approved software for work. Unauthorized downloads can lead to malware infections and create vulnerabilities.

6. **Don't Overuse Personal Devices for Work:**

   - Refrain from using personal email or devices for sensitive work tasks unless explicitly permitted by your IT department.

7. **Don't Disable Security Features:**

   - Avoid turning off or disabling antivirus, firewalls, or security settings, as these are in place to protect your devices and data.

8. **Don't Use Weak or Common Passwords:**

   - Avoid using easily guessable passwords like "password123" or "admin." This increases the risk of unauthorized access.

9. **Don't Delay Reporting Incidents:**

   - Don't hesitate to report any security incidents or accidental mistakes. Prompt reporting can help the organization contain and address potential threats quickly.

10. **Don't Use Public Wi-Fi Without a VPN:**

    - Avoid accessing sensitive information or logging into work accounts on public Wi-Fi unless you're using a VPN to encrypt your connection. Following these guidelines helps to maintain a secure work environment, protects sensitive information, and strengthens the department's defences against Cyber Security threats.

KUMAR JAYANT
ADDITIONAL CHIEF SECRETARY TO GOVERNMENT

//True Copy//

M. Mekala Devi 19/11/2024

SECTION OFFICER

19/11/24

இணைப்பு

அரசுத் துறைகள் மற்றும் அரசு ஊழியர்கள் பணியிடத்தில் இணையப் பாதுகாப்புடன் பணிபுரிவதற்கான கணினிப் பாதுகாப்பு வழிகாட்டுதல்கள்
செய்ய வேண்டியவைகள் மற்றும் செய்ய கூடாதவைகள்

செய்ய வேண்டியவைகள்:

1. **வலுவான கடவுச்சொற்களைப் பயன்படுத்தவும்:**
   - பெரிய எழுத்துக்கள், சிறிய எழுத்துக்கள், எண்கள் மற்றும் சிறப்பு எழுத்துக்களைக் கலந்து உருவாக்கவும் குறைந்தது 8 எழுத்துகள் கொண்டதாக இருக்க முயற்சி செய்யவும்.
   - ஒவ்வொரு கணக்கிற்கும் தனித்தனியான கடவுச்சொற்களை உருவாக்கவும், குறிப்பாக வேலை தொடர்பான கணக்குகளுக்காக.

2. **2-அடுக்குப் பாதுகாப்புடன் இயக்கவும்:**
   - உங்கள் வேலைக்கான கணக்குகளை எப்போதும் 2-அடுக்குப் பாதுகாப்புடன் இயக்கவும், இது உங்கள் கடவுச்சொல் தவறான வழியில் பயன்படுத்தப்படுவதைத் தவிர்க்கக் கூடுதல் பாதுகாப்பு வழங்கும்.

3. **கடவுச்சொற்களை அடிக்கடி புதுப்பிக்கவும்:**
   - குறைந்தது மூன்று மாதத்திற்கு ஒருமுறை கடவுச்சொற்களை மாற்றவும், மேலும் கடவுச் சொற்கள் பிறரால் அறியப்பட்டதாக சந்தேகித்தால், உடனே மாற்றவும்.

4. மென்பொருட்களை புதுப்பிக்கவும்:
   - மென்பொருள், இயங்குதளம் மற்றும் ஆன்டிவைரஸ் ஆகியவற்றை சீரான கால இடைவெளியில் மேம்படுத்த வேண்டும். புதிய அல்லது பழைய பாதுகாப்புக் குறைவுகளைத் தவிர்க்க மென்பொருளின் புதிய பதிப்பைப் புதுப்பித்திடுங்கள்.

5. **வன்பொருள் சாதனங்களைப் புதுப்பிக்கவும்:**
   - பழைய கணினி சாதனங்கள் சமீபத்திய மென்பொருள் பாதுகாப்பு மேம்பாடுகளை ஆதரிக்காது. ஆகையால் மேம்படுத்தப்பட்ட கணினி சாதனங்களைப் பயன்படுத்துங்கள்.

6. **ஆன்டி-வைரஸ் மற்றும் ஆன்டி-மால்வேர் பயன்படுத்துதல்:**
   - இணைய இணைப்புடன் இருந்தால் வைரஸ் தாக்குதல்களை முற்றிலும் தவிர்க்க முடியாது. ஆனால் ஆன்டி-வைரஸ் மற்றும் ஆன்டி-மால்வேர் செயலி/ மென்பொருள் நிறுவுவதன் மூலம் ஆபத்துகளைக் குறைக்க முடியும்.

..2

7. **உங்கள் கணினியில் இருந்து Adware நீக்குதல்:**
   - Adware உங்கள் தனிப்பட்ட தகவல்களைச் சேகரிக்கும். எனவே அவற்றை உங்கள் கணினியிலிருந்து நீக்கவும். Adware cleaner-ஐப் பயன்படுத்தி உங்கள் கணினியிலிருந்து தேவையற்ற மென்பொருள்களையும் Adware-களையும் நீக்கவும்.

8. **சேமிப்பு சாதனங்களை (Pen drive, Hard Disc) ஸ்கேன் செய்யவும்:**
   - வெளியக சேமிப்பு சாதனங்களில் வைரஸ் பரவாமல் இருக்க அவற்றைச் ஸ்கேன் செய்து சரிபார்க்கவும்.

9. **பணியாளர்களுக்கு பயிற்சிகளை வழங்கவும்:**
   - பணியாளர்களுக்கு சைபர் பாதுகாப்புப் பயிற்சிகளை வழங்குவதன் மூலம் பாதுகாப்பு நடைமுறைகளை உறுதிசெய்யுங்கள்.

10. **இணையதள இணைப்புகளை திறக்கும்போது கவனமாக இருக்கவும்:**
    - "திறக்கும்முன் உண்மையான இலக்கைப் பார்க்கவும்" என்பது ஒரு இணைய இணைப்பின் மீது கிளிக்செய்யாமல் (hover செய்து பார்த்து) பார்த்து, இதன் மூலம் அந்த இணைப்பு எங்கு செல்லப்போகிறது என்பதனை நீங்கள் கண்டுபிடிக்கலாம்.
    - நம்பகமான இணைப்பு ஆதாரங்களில் மட்டுமே கிளிக் அல்லது இணைப்புகளைத் திறக்கவும், திறக்கும்முன் இணைப்புகளை வரையறுக்கவும்.

11. **பாதுகாப்பான VPN நெட்வொர்க்குகளைப் பயன்படுத்தவும்:**
    - பாதுகாப்பான, கடவுச்சொல் பாதுகாக்கப்பட்ட Wi-Fi நெட்வொர்க்களுடன் மட்டுமே இணைவது. பொதுப் Wi-Fi-ல் வேலை வளங்களை அணுகும்போது VPN-ஐப் பயன்படுத்தவும்.

12. **ப்ளூடூத்தை தேவையின்றித் திறக்க வேண்டாம்:**
    - ப்ளூடூத் வழியாகவும் ஹேக்கிங் செய்ய முடியும், எனவே தேவையில்லாமல் திறக்க வேண்டாம்.

13. **பயன்படுத்தாத போது சாதனங்களைப் பூட்டவும்:**
    - உங்கள் சாதனங்களை – கணினிகள், மடிக்கணினிகள் மற்றும் தொலைபேசிகள் ஆகியவற்றைப் பயன்படுத்தாத போது Logout செய்யவும். இது உங்கள் தரவுகளை மற்றும் தகவல்களைப் பாதுகாக்க ஒரு முக்கிய படியாகும்.

14. **சந்தேகத்துக்கிடமான செயல்களைப் புகார் அளிக்கவும்:**
    - சந்தேகத்துக்கிடமான செயல்களை IT/TN-CERT Security Team-ல் புகார் அளிக்கவும், உடனடியான புகாரளிப்பு, அபாயகரமான சம்பவங்களைத் தடுக்கும் மற்றும் தகவல்களைப் பாதுகாக்க உதவும்.

15. **தனிப்பட்ட சாதனங்களின் பாதுகாப்பு:**
    - உங்களுடைய தனிப்பட்ட சாதனங்களைப் பயன்படுத்தி வேலை செய்வதை அனுமதித்தால், அவற்றின் பாதுகாப்பை உறுதிசெய்ய, ஆன்டிவைரஸ் பாதுகாப்பு, தொடர்ச்சியான புதுப்பிப்புகள் மற்றும் கடவுச்சொல் பாதுகாப்பு ஆகிய வழிகளை பின்பற்றவும்.

16. **தரவுகளின் பிரதிகளை முறையாக சேமித்தல்:**
    - உங்கள் நிறுவனத்தின் தரவுக் காப்பு கொள்கைகளைப் பின்பற்றி முக்கியமான தரவுகளின் பிரதிகளை வழிகாட்டல்களின்படி சேமிக்கவும். தரவுகள் தவறுதலாக அழிந்து போவதற்கான அபாயத்திலிருந்து பாதுகாக்க இது உதவுகின்றது.

17. **நிறுவனத்தின் கொள்கைகளைப் பின்பற்றுதல்:**
    - உங்கள் நிறுவனத்தின் தகவல் பாதுகாப்புக் கொள்கைகளைப் பின்பற்றுங்கள். இதில் தரவுகளைக் கையாளுதல், மின்னஞ்சல் பயன்பாடு, மற்றும் இணையம் உலாவல் வழிகாட்டுதல்கள் அடங்கும்.

<u>செய்யக் கூடாதவைகள்:</u>

1. **கடவுச்சொற்களைப் பகிரக்கூடாது:**
    - உங்கள் கடவுச்சொற்களை யாருக்கும் பகிரக்கூடாது.

2. **சந்தேகமான links மற்றும் இணைப்புகளைத் திறக்க வேண்டாம் கவனமாக இருக்கவும்:**
    - தெரிந்தவைகளைத் தவிர எந்த சந்தேகத்திற்கிடமான அல்லது நம்பகமற்ற links மற்றும் இணைப்புகளைத் திறக்க வேண்டாம்.

3. **பாதுகாப்பு எச்சரிக்கைகளைப் புறக்கணிக்கக் கூடாது:**
    - பாதுகாப்பு எச்சரிக்களைக் கவனத்துடன் கையாள வேண்டும். உங்கள் ஆன்டி-வைரஸ்/பாதுகாப்பு செயலி தரும் எச்சரிக்கைகளை உங்களால் கையாள முடியாவிட்டால் தகவல் தொழில்நுட்பப் பிரிவிடம் தெரிவிக்கவும்.

4. சாதனம் மற்றும் தகவல்களை unattended–இல் வைக்காதே:
   - உங்கள் சாதனங்கள் மற்றும் தகவல்களைத் (USB drive, e–mails, Pen drive) திறந்து வைத்து அல்லது unattended–இல் வைக்கக் கூடாது.

5. **அங்கீகரிக்கப்படாத மென்பொருள் அல்லது செயலிகளை நிறுவக் கூடாது:**
   - வைரஸிடமிருந்து பாதுகாப்பற்ற, அங்கீகரிக்கப்படாத மென்பொருள் (Install) அல்லது செயலி ஆகியவற்றை நிறுவக்கூடாது.

6. உங்கள் தனிப்பட்ட சாதனங்கள் (USB Pen Drive, Laptop) அலுவலக பயன்பாட்டில் உபயோகப்படுத்தக் கூடாது.

7. **பாதுகாப்பு அம்சங்களை செயலிழக்கச் செய்யக்கூடாது:**
   - உங்கள் செயலி மற்றும் தரவுகளை பாதுகாக்க ஆன்டி–வைரஸ், firewalls மற்றும் பாதுகாப்பு அம்சங்களை செயலிழக்க (turning off / disabling) செய்யக்கூடாது.

8. **எளிதில் கணிக்கக்கூடிய கடவுச்சொற்களை பயன்படுத்தக் கூடாது:**
   - பொதுவான வார்த்தைகள், சொற்றொடர்கள், அல்லது எளிதாக கிடைக்கும் தனிப்பட்ட தகவல்களை உங்கள் கடவுச்சொற்களில் தவிர்க்கவும்.

9. **தாக்குதல் நிகழ்வுகளை தாமதமின்றி தெரிவிக்கவும்:**
   - எந்தப் பாதுகாப்பு சம்பவங்களையும் மக்களிடம் தெரிவிக்கத் தயங்காதீர்கள், விரைவான தகவல்தரல் அந்த சம்பவத்தை விரைந்து கண்டறிந்து, எதிர்மறை விளைவுகளைத் தடுக்க உங்கள் நிறுவனத்திற்கு உதவுகிறது.

10. **VPN இன்றிப் பொது Wi–Fi–ஐ பயன்படுத்த வேண்டாம்:**
    - பொது Wi–Fi–இல் VPN பயன்படுத்தாமல் சென்சிட்டிவ் தகவல்களை அணுகவோ அல்லது வேலைக்குத் தொடர்பான கணக்குகளில் உள்நுழைவதைத் தவிர்க்கவும். VPN பயன்படுத்தினால், உங்கள் இணைப்பு குறியாக்கம் செய்யப்படும், இது தகவல்களைப் பாதுகாப்பாக வைத்திருக்கும்.

இந்த வழிகாட்டுதல்களைப் பின்பற்றுவதன் மூலம் உங்கள் கணினிப் பாதுகாப்பு நிலையை மேம்படுத்தி, தனிப்பட்ட மற்றும் நிறுவன தகவல்களைப் பாதுகாக்க முடியும். தரவுகள் பாதுகாப்பாக இருக்க உதவிடும், மற்றும் தொழில்நுட்ப அபாயங்களைக் குறைக்கவும் உதவுகின்றது.

குமார் ஜயந்த்
அரசு கூடுதல் தலைமைச் செயலாளர்

//உண்மை நகல்//

மு.மேகலா தேவி
19/11/2024
பிரிவு அலுவலர்
19/11/24