

OFFICE OF THE JOINT DIRECTOR (IT)  
ROOM NO.7001, 7<sup>th</sup> FLOOR, PALIKA KENDRA  
SANSAD MARG, NEW DELHI-110001  
Office Telephone: 011- 415013673 Ext. 2240

IT SECURITY ADVISORY

No 314660 /Jt.Dir (IT)/2020

Dated: 19/2/2020

It has come to the notice of IT Department that NDMC employee mail id/Payslip and others password is not changed by the user on time to time, because of that the information may be accessed by someone else ,resulting which the data may be shared by others.

In this connection the user has to change the password of following services on periodic basis (15 days) for the safety of their own data.

1. The Official e-Mail Password needs to change on periodic basis (15 days) and always use the hard password in combination of uppercase letters, lowercase letters, numbers and special characters. Please doesn't share the password to other one for the safety of data.

2. The password of Pay-slip needs to change on periodic basis (15 days) and always use the hard password in combination of uppercase letters, lowercase letters, numbers and special characters .Please doesn't share the password to other one for the safety of personal details.

3. The Officers/Official of NDMC should also need to change the password of eFinance, CCB, WAM, Property Tax and other applications on periodic basis (15 days) which is used for day to day work.

IT Security DOS and DON'Ts

Cyber security is the shared responsibility of every employee and organization, which plays a key role in properly safeguarding and using private, sensitive information and state resources. The following Do's and Don'ts help to remind us all of actions we must take to remain vigilant.

**1. Don't be tricked into giving away confidential information:**

Don't respond to emails or phone calls requesting confidential company information— including employee information, financial results or company secrets. It's easy for an unauthorized person to call us and pretend to be an employee or one of our business partners. Stay on guard to avoid falling for this scam, and report any suspicious activity to IT and protect your personal information just as closely.

**2. Don't use an unprotected computer:**

When you access sensitive information from a non-secure computer, like one in an Internet café or a shared machine at home, you put the information you're viewing at risk. Make sure your computer is running the latest approved security patches, antivirus and firewall. And you should work in user mode, not administrator mode, whenever possible

**3. Don't leave sensitive info lying around the office :**

Don't leave printouts containing private information on your desk. Lock them in a drawer or shred them. It's very easy for a visitor to glance down at your desk and see sensitive documents. Keep your desk tidy and documents locked away. It makes the office look more organized, and reduces the risk of information leaks.

**4. Lock your computer and mobile phone when not in use :**

Always lock your computer and mobile phone when you're not using them. You work on important things, and we want to make sure they stay safe and secure. Locking your phone and computer keeps your data and contacts safe from prying eyes.

**5. Stay alert and report suspicious activity**

Always report any suspicious activity to the IT team. Part of our job is to Stop cyber attacks and to make sure Our data isn't lost or stolen. All of our jobs depend on keeping our information safe. In case something goes wrong, the faster we know about it, the faster we can deal with it.

**6. Password-protect sensitive files and devices:**

Always password-protect sensitive files on your computer, USB, smartphone, etc. Losing items like phones, USB flash drives and laptops can happen to anyone. Protecting your devices with strong passwords means you make it incredibly difficult for someone to break in and steal data.

**7. Always use hard-to-guess passwords :**

Don't use obvious passwords, like "password," "cat," or obvious character sequences on the qwerty keyboard, like "asdfg" and "12345." It's better to use complex passwords. \* Include different letter cases, numbers, and even punctuation. Try to use different passwords for different websites and computers. So if one gets hacked, your other accounts aren't compromised.

**8. Be cautious of suspicious emails and links :**

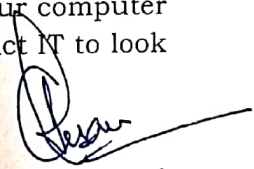
Don't let curiosity get the best of you. Always delete suspicious emails and links. Even opening or viewing these emails and links can compromise your computer and create unwanted problems without your knowledge. Remember, if something looks too good to be true, it probably is.

**9. Don't plug in personal devices without the OK from IT :**

After the deployment of policy based Active Directory(which is in process), personal devices like USB flash drives, MP3 players and smartphones etc. needs to be validated by IT Department before the use . These devices can be compromised with code waiting to launch as soon these are plugged in to a computer. Talk to IT about your devices and let us make the call.

**10. Don't install unauthorized programs on your work computer**

Malicious applications often pose as legitimate programs, like games, tools or even antivirus software. They aim to fool you into infecting your computer or network. If you l' application and think it will be useful, contact IT to look into it for you before installing.



**A.W. Ansari**

**Joint Director(IT)**

Copy to:

1. PS to Chairman for information please.
2. PS to Secretary for information please
3. PS to Financial Advisor for information please
4. PA to Director (IT) for information please
5. Head of Departments
6. Notice Board