Information Security Guidelines for Working from Home

ජනාධිපති කාර්යාලය
சனாதிபதி அலுவலகம்
Presidential Secretariat

SRI LANKA CERT|CC

With the transition to working from home, there is an increase in information security threats.
Please adhere to the following do's & don'ts all the time to work securely and safely from home.

Issued: 10th November, 2020

Files & information

- Keep all official documents under lock and key when unattended.
- When disposing of confidential documents, always shred or tear them into tiny pieces to prevent unauthorized persons obtaining them.
- Do not share or upload official sensitive information to public and open web sites and storage sites.
- Share data, information and files only on a "need to know" basis.
- Obtain a backup of important files at a regular schedule and store them in a secure manner.
- Use all official data, information and files only for the intended purpose.

Email, text & websites

- Do not use your official email ID to register to receive news and any other non-work related information.
- Do not download or install suspicious, illegal or third-party unauthorized software, apps or games.
- Do not click on links or download attachments in emails or text messages from unknown/suspicious senders.
- Be careful with any emails referencing COVID-19 or free data, as these may be phishing attempts or scams.
- Do not browse unsafe websites (e.g.: games, gossip sites, gambling sites, pornography, etc.)

Computers, smart phones or tablets

- Avoid using unknown public Wi-Fi hotspots for work.
- Report any lost devices that contain official information to the authorities immediately.
- Never use unknown pen drives/thumb drives. In case you need to use one, make sure to scan it with a legitimate/licensed antivirus tool.
- Install a legitimate/licensed antivirus tool from a well-known provider on your device and keep it regularly updated.
- Shutdown your computer when not in use. It is your responsibility to safeguard government provided equipment.
- Where possible, encrypt the contents of your hard drive. This ensures that sensitive confidential data will not be exposed to outside parties in the event your device is lost or stolen.
- Always update your operating systems and software with the latest patches. e.g. operating system, antivirus signatures, browsers, add-ons
- Create a user without admin rights on your machine to use for day-to-day work. Avoid using a user with admin rights for day-to-day work.
- If you have been provided with an official secure connection facility such as a VPN, use only that to connect to work systems.
- Always disconnect VPNs when not in use
- Never leave devices unattended. Always lock your devices when unattended.

Passwords & credentials

- Change your passwords frequently.
- Use strong passwords, passphrases or PINs for all your devices / applications and always keep devices locked when not in use.
- Don't write passwords on pieces of paper or notebooks.
- Use a password or passphrase that is easy to remember and hard to guess. Avoid using simple passwords.
- Whenever possible, use two factor authentication for added security.
- Never share your password or OTP (One Time Password) with anyone. You are accountable for any action performed using your credentials.
- Do not share your personal information over email, websites, social media platforms (WhatsApp, Imo, Facebook, etc.) or a phone call.
- Avoid reusing offical passwords on applications or websites used for personal use.
- Secure your home Wi-Fi with a strong password.

Reporting & help

- Read, understand and strictly adhere to your organization's information security policies. When in doubt consult your supervisor or your department head.
- Report any suspicious activities on your devices to the relevant IT personnel and/or your department head.
- Report any security incident immediately to your department heads and to incidents@cert.gov.lk.