Updated March 26, 2020

Work from Home Securely: Guidance for Contingent Workers

Best practices to help safeguard Intel's information while working from home

This Guidance should be used in conjunction with completing and adhering to policies in the Information Security Awareness for Contingent Workers training courses: 2020 Information Security Awareness or Information Security Awareness for ODC Workers and existing applicable Intel Information Security policies.

With an increase of Intel contingent workers working from home, it's even more important to continue secure behaviors beyond Intel. Use the following best practices to help reduce risks to Intel's information.

Use only Intel-provided or Intel-managed equipment for work

This includes laptops and mobile devices issued by Intel to use at work. Remember:

- Devices and files need to be protected in-transit. Securely transport information and devices, and don't leave sensitive information or devices visible in your car.
- Get clearance from your company manager and Intel sponsor before bringing Intel resources home.
- At all times, stay within this Intel guidance and any guidance provided by your company.
- Under exceptional circumstances, if you have a personal mobile device that you have been asked by Intel to use for work, contact your sponsor to ensure your device is registered with Intel mobile access services.

Connect securely

- **Use Restricted VPN, VPN** or Office 365 (if enabled) to access Intel's corporate network and resources.
- **No Remote Desktop connections.** Connecting to your work system from a home system is not permitted. This includes logging into your work PC using any device that is not Intel managed, provided, or approved. Using unapproved tools for remote connections violates Intel Information Security policy and is prohibited.
- **Avoid using public Wi-Fi networks** that may be accessible from your home, use a trusted connection.
- Make sure your home network devices have the latest software patches and security configurations.
  - If you have a wireless router, follow best practices* to make it more secure.
  - *Recommended*: Search in the instructional guide for each of your personal home network devices for instructions on updating its password, software, and firmware.
- As more of us work from home, Intel IT is bolstering our cyber defenses by tightening controls and increasing VPN capacity and monitoring. While using Intel's VPN, you're connected to Intel's network, which is being carefully monitored for load balancing and security purposes. It's important to minimize web activities that can increase your cyber risk exposure.

Collaborate securely

Only use Intel-approved collaboration solutions. Remember these tips:

- **Be aware of social application limitations.** While free social and texting apps may help us stay connected, never discuss, exchange, or share Intel Confidential or Intel Top Secret information over apps like Viber, WhatsApp, WeChat, Messenger, or any app not approved for sharing classified information.
- **Follow policy.** Intel's corporate and information security policies prohibit downloading any classified (non-public) information to devices, platforms, or cloud solutions not previously approved by Intel.
    - If you have additional equipment you've been authorized to take home, check with your company manager or Intel sponsor before using it to work with Intel classified information.
- **Don't overshare.** With an increase in social media sharing of information, it's even more important to be aware of what you share. If in doubt, leave it out.

Compute securely

Practice safe computing
Exercise extra caution when using Intel assets outside the office:

- Only use trusted applications and services and allow Intel to update your system. Some websites and services, even legitimate ones, host malicious code or ads that display phony update alerts. Clicking them could install malware.
- Report any suspected malware, alternatively, **contact your Intel sponsor immediately**. If malware is detected on your Intel system, you will be alerted by IT Information Security.
- With pandemic-related restrictions in place, getting your system rebuilt has new challenges. For Intel IT-supported devices, you may be directed to work with IT.intel.com or your local Intel IT Service Center to determine the appropriate resolution within the new parameters.
- When you're about to step away from your computer, lock your screen. If it is going to be out of your sight for a long time, shut it down or place it in hibernate to enable hard drive encryption.
- Avoid printing documents when possible, make sure loose papers are out of sight and secure, and properly dispose of any printed work material by shredding or storing securely until you can dispose of it properly.
- **Enable security and updates.** Do not disable Intel security software on your devices and always comply with Intel IT update or patching notifications.
- Don't turn off security services such as McAfee Endpoint Security, McAfee Agent, or Sandblast Protect.
- As always, please work with your company for securing additional productivity or ergonomic equipment that may be needed to support working from home more effectively.

Stay vigilant
The world is seeing an increase in phishing and other scams related to the pandemic and working from home. Be alert to suspicious messages (email, texts, and voicemail):

- When looking for information, always visit trusted sources such as the Intel updates on the coronavirus posted on supplier.intel.com / evolving updates and FAQs for supplier on supplier.intel.com or the World Health Organization* (WHO) or your company, as well as Circuit if you have access within the firewall.
- Cybercriminals are using concerns about the pandemic to spread malware.
- If a message is suspicious or unexpected, verify that the source is legitimate, resist clicking on links or opening attachments, and report suspicious messages. Learn more at Microsoft Threat Protection.
- Report any suspicious activity to secure.intel@intel.com.

Thanks for helping keep Intel information secure!
