Wednesday, June 3, 2020

Telework Security and Privacy Reminders

Information security is everyone's responsibility. As we continue to work remotely, please be reminded of the following guidelines to keep the County Assets (e.g., Non-public Information, devices) protected. We must remain diligent to protect ourselves and the County.

Remote Desktop Tools

- Use **Zscaler** if you are using a County-issued device.
- If you are using a personally-owned device, use **AppStream**.
- MyPC VDI will be decommissioned in July 2020.
- County Non-public Information MUST NOT be saved on personally owned devices (e.g., desktop/laptop/tablet/mobile device, USB flash drives).
- When there is a business reason to save County Non-public Information to an USB flash drive, only DHR-issued encrypted flash drive may be used.
- County Non-public Information MUST NOT be saved on public online storage (e.g., iCloud, Google Docs).

File Sharing, Collaboration and Teleconferencing Tools

- Microsoft Teams is a collaboration app that helps your team stay organized and have conversations, all in one place (e.g., Chat, File Share, Meeting, Audio/Video Calling capability).
- Microsoft OneDrive for Business can also be used for secure online file storage and sharing.
- Only use County approved teleconferencing tools such as Teams, Cisco WebEx.

Email Communication

- County Non-public Information MUST NOT be sent to personal email account.
- There must be an approved business reason to send County Non-public Information in email and the message must be sent securely by inserting '**[Secure]**' in the email subject line.
- Be suspicious of any unsolicited email requesting personal information. When in doubt, click the "Report Phishing" button in Outlook.

Printing

- Printing can expose County information. You must have prior management approval for printing. Printed documents must be stored securely.
- Documents containing County Non-public Information are prohibited from being printed on personal printers.
- When disposing of the printed documents, you must use a “cross-cut” shredder to dispose of it securely.

Questions/Reporting Issues

- Potential security or privacy incidents including lost or stolen computing devices used for County business, regardless of County or personally-owned, MUST BE reported immediately to DHR DISO at DHR-DISO@hr.lacounty.gov .
- For questions concerning County approved telework and collaboration tools, contact DHR IT Support at dhritsupport@hr.lacounty.gov .

Additionally, please do complete the countywide mandatory information security awareness training modules, if you have not already done so. These training modules provide useful information on common security and privacy best practices, cybersecurity threats and how to address such threats.