Work from Home: Information Security – March 18th, 5PM

The contents of this document are made available to you for informational purposes only and should not be construed as legal, financial or medical advice on any matter. This material may not reflect the most current COVID-19 developments and is subject to revision. In no event will Business Leaders for Michigan be liable for any decisions made or action taken in relation upon the information provided through this document.

Description of issue: As employees are asked to work from home, they are still handling sensitive or proprietary information. It may be helpful to remind your employees some best practices to ensure proper managing of information.

General best practices:

- Share what constitutes sensitive of proprietary information
- Provide a list of safeguards employees can deploy
- Provide a place for employees to ask questions if they occur

Detailed sample communication below:

Sample A:

INFORMATION SECURITY GUIDANCE

FOR FLEXIBLE / AGILE WORK

(Note: This represents our global guidance; follow more specific regional and functional guidance as applicable.)

Working outside of company offices requires special care to protect confidential and sensitive business information. Employees must at all times follow company policies and processes for confidential information, privacy, data security and information management.

Information Security Starts With Awareness

Many employees handle confidential and sensitive information on a daily basis, including:

- **Non-public business and technical information** including strategies, plans and communications;
- **Financials** including material non-public information;
- **Personally identifiable information** ("PII") of our employees, consumers or others;
- **Intellectual property** and trade secrets;
- Confidential information entrusted to the company by our **trade customers** and **suppliers**; and
- Privileged **legal** correspondence with our Law teams.

Safeguards When Working Outside The Office

Employees must take care when working outside the office to protect company information from being lost or misused. Basic safeguards include:

- **Conversations** and phone calls involving sensitive information must be held in private locations.
- It's recommended that you use your **company-provided device** while working offsite. Do not leave company devices in unattended vehicles or other places where they may be stolen. Immediately report lost or stolen devices to IT and/or Security.
- If it's necessary to use a personal device, follow company IT guidelines including approved software and security protocols. Do not download or store company business records on personal devices.
- Use **company email** to conduct company business; never use personal email accounts to transmit sensitive or privileged company information.
- **Paper business records and files** must be secured at all times and managed according to company retention policies and applicable legal holds. Shred or destroy sensitive documents that are discarded.

How To Get More Information

Please direct questions to your supervisor or a representative of IT, Law or HR. Also refer to applicable company policies.