PROTECTING CONFIDENTIAL INFORMATION
WHEN WORKING FROM HOME OR REMOTELY

- Take necessary precautions to secure all Department equipment and confidential information in your possession by minimizing the risk of damage, theft and unauthorized access.

- When possible, confidential information that is brought home, shall be immediately placed in a secure location. When possible, secure hard copies of confidential information in a locked cabinet, drawer, briefcase or door to the room when not in use. Ensure that non-employees do not access Department data, either in print or electronic form.

- Do not leave laptops, mobile devices, records and other information unattended in an unsecured vehicle.

- Do not remove records and information from the Department unless approved in advance by your supervisor, and limit records and information to what is necessary to conduct the Department's business. Records must be returned to the Department upon conclusion of the need to conduct work at home or remote location.

- Remote access to confidential information and is only allowed through a secure VPN connection. Any connection from an open wireless network is prohibited unless a secure VPN connection is used. All access to outside systems or networks is prohibited unless there is a secure encrypted connection and it is approved by the Department.

- Do not connect personally-owned laptops and mobile devices to the State network without the approval of the Department and NDIT. Do not access, save, store, transmit, or receive confidential information on a personally-owned laptop or mobile device unless approved by the Department and NDIT.

- Only access, use and disclose information via Remote Access as minimally necessary to perform your duties. All confidential information is to be saved on the secure servers, and not on the computer's local drive.

- Log-off and disconnect from Department's network when access is not needed to perform job responsibilities.

- Protect laptops and other mobile devices by using passwords. Do not record or write down passwords where unauthorized persons might discover them.

- Virus Protection software is installed on all Department computers and is set to update the virus pattern on a constant basis. Do not stop the update process for Virus Protection on your work laptop or mobile device.

- Notify the Department immediately of any suspected breach that compromises or could compromise the security of confidential information.

- If you suspect infection by malware, immediately stop using the computer or mobile device and immediately contact the NDIT Service Desk. Do not use CD-ROMS, USB drives, diskettes or other magnetic storage media used by the infected computer or mobile device must not be

used with any other computer or device until the malware has been successfully eradicated. Immediately isolate the infected computer or device from internal networks. Do not try and remove the malware.

- All emails containing confidential information sent outside the Department's email system (nd.gov) must be encrypted. Unencrypted messages between Department employees or Department employees and providers shall not contain confidential information.

- If you maintain a telephone line, cellular or landline, furnish your supervisor with the number.

- Confidential information may be shared over the telephone in the same manner that it may be released in person, in accordance with the applicable federal and state laws, federal regulations, administrative rules, and Department policies. When discussing confidential information over the phone, take precautions to ensure that you are not overheard by family members and others in the home.