UCSB Cybersecurity Checklist for Telecommuting & Remote Work

The employee is responsible for ensuring cybersecurity as a condition of approval to telecommute or working remotely. The employee should be provided this checklist electronically prior to the start of telecommuting or working remotely.

☐ All electronic communication must comply with the relevant University's Internet Technology Policies and Guidelines, including the Electronic Communication Policy.

☐ The employee must review and follow UC policies and procedures pertaining to the handling of public, University and student records.

☐ Any computer, whether personal or University-owned that is used by the Employee for University work should be configured according to University and the individual department's IT standards, including the following:

- Anti-malware and firewall software installed and configured to automatically update.
- Operating system and all installed software kept updated directly from software vendors on a timely basis.
- Full-disk encryption configured and used.
- Day-to-day activities conducted using a non-privileged account (i.e. not a member of the local admin or domain admin group)
- University data may not be stored on removable devices without encryption

☐ Where a wireless connection is used, gateway should be configured to use WPA2PSK with a key > 14 characters. The use of open Wi-Fi should be avoided, and if required, a VPN must be used for all activities. Information on the campus VPN can be found at http://www.ets.ucsb.edu/services/campus-vpn.

☐ Voice over IP telephony (VolP) and/or video conferencing should be conducted over VPN or using secure protocols.

☐ Flash drives or other portable drives must be scanned for viruses before being used for uploading or downloading data.

☐ Ensure protection of University data on disk, hardcopy, or on portable devices from theft, loss, or unauthorized access during transit.

☐ All work must be backed-up. Authorized cloud storage services such as Box or Google Drive may be used to back-up files that do not include sensitive personally identifiable information or personal health information. If removable media is used for backup, it must be encrypted.

☐ Employee understands the importance of system security and agrees to promptly inform the supervisor when/if security matters arise. Security incidents, including loss or theft of equipment, must also be reported according the processes outlined at https://security.ucsb.edu/. Sensitive information in hardcopy form must be returned to the department or shredded

☐ Employee acknowledges and understands that any computing equipment used for University business purposes, whether personal or University owned, may be subject to discovery and production of records pursuant to the California Public Records Act.

Employee Name: _____Title: _____

Employee Signature _____Date: _____

Version: 10/23/2017

Retention: Signed checklist should be maintained in the employee's departmental personnel file along with the signed UCSB Telecommute-Remote Work Agreement.