A Project of
TechForce Hawaii

COVID-19 LONG-TERM TELECOMMUTING FOR SOCIAL DISTANCING

TELECOMMUTING & CYBERSECURITY CHECKLIST (5/26/20)

The following checklist has been prepared to assist employers in developing a telecommuting program to respond to the social distancing and isolation needs in responding to COVID-19. The checklist utilizes guidance and information provided by the DHS Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), the National Initiative for Cybersecurity Education (NICE), and the Federal Communications Commission (FCC).

It is not legal or information technology (IT) advice. Check with your legal counsel, Human Resources, and IT advisors before finalizing your Telecommuting Program.

STEP 1: DETERMINE TELECOMMUTING PROGRAM PARTICIPATION

- **For each worksite/office, division/department, and team/crew determine the following:**

  - □ Which employees will continue/resume full-time work in-office? Which employees will continue to telecommute?
  - □ Will employees be allowed to choose to telecommute, and will you consider factors such as:
    - Workers with individual risk factors (e.g. age 65 or older; chronic medical conditions, including respiratory and immunocompromising conditions; pregnancy);
    - Workers who need to care for child due to schools or day-care centers being closed; and
    - Workers with household members who have individual risk factors and/or COVID-19.

- **Decide whether the program will have a predefined end or date of review (e.g. lifting of stay-at-home orders).**
- **Determine authorizations needed and develop documentation for participation**. If employees are allowed to choose to telecommute as an accommodation or through some other criteria, decide how you will verify need.

STEP 2: DEVELOP SCHEDULES, WORKFLOW AND COMMUNICATIONS PROTOCOLS

- **Determine schedules and work times based on operational needs and wage and hour constraints**

  - □ Will telecommuters work normal business hours, be offset from in-office workers, or some other schedule?
  - □ Consider wage and hour requirements for non-exempt employees. Such hourly workers must be compensated for:

- ▪ All time they are required or permitted to perform work, INCLUDING responding to calls or emails during “off-hours”
- ▪ All mandatory meetings, training, and online conferences
- ▪ All hours worked over 40 hours per work week

□ Consider workload and wage and hour requirements for exempt employees:

- ▪ Do they have enough work to justify salaries, or would a temporary change to hourly make more sense?
- ▪ Minimum guaranteed salary is $35,568/year to qualify as exempt

➢ **Determine whether timekeeping practices must be adjusted for telecommuters**

□ Submission of time sheets for non-exempt workers
□ Prior approval of overtime work
□ Recording meal breaks
□ Leave practices for errands, home schooling, other personal obligations

➢ **Establish communications protocols**

□ Schedule regular check-ins between supervisors and direct reports
□ Identify best methods for casual and formal communications
□ Set protocols for communicating special authorizations (e.g. purchases, fund transfers, collecting or granting access to sensitive information)
□ Adjust methods for performance management or supervision of telecommuting employees
□ Hold employees and supervisors accountable

➢ **Adjust workflows for telecommuters**

STEP 3: EVALUATE EXISTING EQUIPMENT AND PRIVACY/SECURITY SYSTEMS

➢ **Inventory devices and systems**

□ Physical devices and equipment (employer- and employee-owned with access to organization systems, removable storage media)
□ Software platforms and applications
□ Networks and communication
□ External information systems (cloud storage, data centers, etc.)

➢ **Inventory access control procedures and tools and determine whether changes are needed**

- □ Identify procedures, documentation, and tools to grant, manage, and revoke physical access to facilities and equipment
  - Keys,
  - "Lock out/tag out" protocols
  - ID verification systems (badges, biometrics, in-person verification etc.)
  - Network segmentation
  - Logs of assignment, use, return

- □ Identify procedures, documentation, and tools to issue, manage, verify, revoke, and audit access to devices, systems, and information
  - Credentials (usernames and passwords) and authentication (multifactor?)
  - Minimum specifications (see below)
  - Administrative controls
  - Network segmentation
  - Employee lifecycle procedures (onboarding, privilege changes, out-processing)
  - Backup and destruction processes

➢ **Identify key personnel and roles**

- □ User groups and security classes
- □ IT helpdesk and frontline response
- □ Administrators and executive decision makers
- □ Custodians of record(s)
- □ Privacy/security officers (if applicable – see Step 4 regarding specialized privacy/security needs imposed by law)
- □ Emergency points of contact

STEP 4: DETERMINE PRIVACY/SECURITY NEEDS AND PROTECTIONS

➢ **Determine privacy and security requirements**

- □ Determine whether you handle protected classes of information and/or service clients/customers with special legal protections or requirements
  - Protected Health Information (PHI)
  - (Nonpublic) Personal Identifying Information (PII)
  - Credit and financial information
  - Employee investigations
  - Defense-sensitive information re controlled technologies
  - Critical infrastructure

- Student records
- Minors

□ Take stock of what obligations you have by contract/agreement

- Nondisclosure/confidentiality agreements
- Service or supply agreements
- License, royalty, or other proprietary rights agreements

□ Take stock of information your organization wants to keep protected from public disclosure

- Intellectual property (trade secrets)
- Other nonpublic information company wishes to keep confidential (e.g. financials, login credentials, salaries, etc.)

➢ **Determine whether existing procedures or technological controls are sufficient to protect information throughout "data lifecycle," considering:**

□ Collection

- Informed, affirmative consents & documentation
- Notices re passive collection (e.g. website analytics)

□ Use and processing

- Restrictions by context of collection

□ Storage

- Is sensitive information segregated from other information?
- Short-term vs. long-term storage (backups, archival, etc.)

□ Transfer, sharing, and distribution

- Secure transfer needs (email encryption, mass file transfer)
- Registration of intellectual property
- Labeling conventions
- Nondisclosure agreements or similar contractual controls

□ Return or destruction

➢ **Set minimum specifications for employee device use with employer systems**

□ Operating systems and software versions
□ Update and patch schedules
□ Utilization of security features (e.g. lock screens)
□ Restrictions and controls on sharing devices with non-employees

- □ Restrictions on network use and configuration
  - ▪ Unsecured public networks allowed?
  - ▪ Minimum specifications on home networks?
  - ▪ VPN, mobile data, other tools?

- □ Restrictions on user modification
  - ▪ No "jailbreaking" or circumvention of control features
  - ▪ No modification of proprietary software

- □ Restrictions by device/service type – may require individual review of security features and configurations
  - ▪ "Smart" devices, IoT, virtual assistants
  - ▪ Bluetooth and other near-field communications (NFC) enabled devices
  - ▪ Removable media (external hard drive, USB/flash storage, disks, SD cards, etc.)

- □ Reporting of tampering, loss, or theft

➢ **Determine whether procedures and controls must be modified based on privacy/security needs and remote working needs**

- □ Do access controls/authentication processes require in-person contact?
- □ Are access controls/credentials shared or duplicated between users?
- □ Are existing procedures viable in the event an employee suddenly becomes unreachable?
- □ Are procedures recorded in writing and have they been provided to telecommuters?
- □ Do the employee handbook or other policies inform telecommuters of increased monitoring while working from home?
- □ Are there sufficient monitoring and intrusion detection safeguards in place?
  - ▪ Facilities and physical assets monitored?
  - ▪ Network activity and remote access monitored?

➢ **Evaluate pandemic-related risk factors and buying considerations**

- □ Cost of investment vs. cost of noncompliance/breach remediation
- □ Is your organization part of critical infrastructure or essential business supply chain?
- □ Does your organization provide or support direct community relief or economic recovery?
- □ Is your organization the only goods/service provider of your kind within your community?
- □ Are resources and/or service provider availability affected by or likely to be affected by the pandemic?

STEP 5: EVALUATE OR DEVELOP EMERGENCY RESPONSE AND RECOVERY PLANS

- **Determine whether breach or other emergency response plans must be modified to prepare for increased remote working**

  - □ How will communication and coordination of response team be affected?
  - □ How will information gathering from, and direction and control of remote users be affected?
  - □ Are existing controls (see above) sufficient to contain incidents?

- **Determine whether recovery plans must be modified for remote working and social distancing**

  - □ Are recovery resources (outside consultants, services, materials, etc.) available?
  - □ Can coordination of recovery efforts be done remotely?
  - □ Will required notifications (see above re privacy/security requirements) be affected by remote working?

- **Determine whether your organization is adequately insured**

  - □ Review exclusions from general liability, umbrella, business interruption and EPLI policies
  - □ Review cybersecurity policy (if applicable) for required prevention and response measures
  - □ Review additional resources available for response and recovery provided by insurer

STEP 6: COMMUNICATE POLICIES AND PROCEDURES

- **Prepare written summaries of the following policies and procedures and provide to employees:**

  - □ Telecommuting Policy
    - Authorizations needed
    - Operational, technical, and accommodation requirements
    - Communications expectations and practices
    - Timekeeping practices
    - Safety reminder & reporting

  - □ Acceptable Use Policy
    - Cross-reference Employee Handbook provisions re remote monitoring
    - Device & security requirements
    - Restrictions on use of company equipment, systems, and information

  - □ Privacy/security obligations and procedures for dealing with controlled information and access
  - □ Emergency plans

- ▪ Procedures for employees reporting problems or concerns (injury, loss/theft/intrusion to systems)
- ▪ Procedures for notifying employees about emergency situations

➢ **Train employees on cybersecurity practices**

- □ How to spot "red flags" and avoid phishing, scams, and other exploits
- □ Communications and authorizations policies
- □ Breach response, contact persons, and communications

➢ **Prepare written notices of communications practices as needed for your:**

- □ Vendors, suppliers and other business associates
- □ Clients/customers

ADDITIONAL RESOURCES:

CISA Resource Hub: https://www.cisa.gov/cyber-resource-hub
NIST Cybersecurity Resources: https://www.nist.gov/cyberframework/general-resources
NIST Cybersecurity Framework: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
FCC Small Biz Cyber Planner: https://transition.fcc.gov/cyber/cyberplanner.pdf
Center for Internet Security Controls & Resources: https://www.cisecurity.org/controls/cis-controls-list/