

Telecommuting for Law Firms

An Implementation Manual

- ✓ **Telecommuting Policy**
- ✓ **Safety and Workers Compensation**
- ✓ **E-mail and Voice Mail Policy Considerations**
- ✓ **Sample Telecommuting Agreement**
- ✓ **Security Policy Checklist**
- ✓ **Other Resources**

Telecommuting Policy

A good telecommuting policy will provide your firm with clear, consistent guidelines. The policy should be broad enough to allow individual work groups to customize it.

It is recommended that the Human Resources Department or Personnel Department steward the development of the policy. A draft policy can be submitted to practice groups or local office managers for review and customization.

Law firms should treat telecommuting as any other term and condition of employment. The procedures, which govern the relationship, should be clearly set out in writing. Naturally, the language of a telecommuting policy will vary from firm to firm, depending on the nature of a firm's practice and competitive conditions in the local labor market. The following items should be addressed in any telecommuting policy, regardless of the firm's particular situation:

- Define telecommuting
- Make it clear that telecommuters are still subject to the firm's employment policies and procedures
- Set out the work hours and days for telecommuters
- Advise telecommuters that the employer retains the right to cancel the telecommuting arrangement at any time, without cause or advance notice
- Assign the telecommuter responsibility for maintaining a safe workplace and an ergonomically correct work station
- Grant the Firm the right to inspect the telecommuter's work area and state when such inspections can occur
- Reaffirm that the employer's workers' compensation insurance applies to telecommuters and require telecommuters to immediately report work-related injuries
- Explain where telecommuters can hold business meetings

- Assign liability for any injuries to third parties which occur in the telecommuting work place
- Detail what equipment the telecommuter will be using, who will be providing it, who is responsible for maintaining it, where the equipment will be located, who is responsible for loss or damage to the equipment, and for insuring it, and when any Firm-owned equipment must be returned to the Firm if the employment relationship ends
- Impose upon the telecommuter a duty of confidentiality and set out any procedures telecommuters must follow to ensure that confidentiality
- Require telecommuters to immediately report to the employer any acts of workplace harassment or violence

Safety

Employees working at home or at remote locations remain protected by state workers' compensation laws, as well as applicable federal and state occupational health and safety regulations. For California employers, the health and safety arena includes the state's ergonomics law.

Employers are legally obligated to provide their employees with a workplace that is free from hazards that might cause serious harm or injury. To meet this obligation, an employer might even need to periodically inspect the telecommuter's "office." If so, personnel policies should clearly set out the hours and days when such inspections can occur, and identify by title or position which firm personnel can be expected to make such inspections. As an alternative to site visits, some employers require the employee to provide a clear photo of the area to be used for telecommuting.

An initial inspection at the beginning of the telecommuting relationship might be performed so the employer can identify any unsafe conditions in the workplace, and assist the employee in responding to such conditions. The employer should also impress upon the employee the importance of maintaining a safe workplace and educate the employee with respect to what it will take to do so.

In some states, a workers' compensation injury can include any injury arising out of the employment relationship. Employers with a telecommuting workforce run the risk of not knowing if a workers' compensation claim truly resulted from a work-related injury or some other event. Requiring employees to log in and out regularly may help pinpoint whether the activity at issue was work-related or not. Employers should also require employees to report work-related injuries and submit to an immediate workplace inspection. Obtaining an explanation of exactly what occurred at the accident site will enable the employer to fully and fairly investigate claims.

Email and Voice Mail Policy Considerations

For those employers who do not yet have an email/ voice mail policy in effect, the "before" policy which follows may seem a bit futuristic. However, this policy is rapidly becoming outdated. Due to the meteoric rise in the popularity and use of the Internet, as well as the recent trend in lawsuits over Internet and email related abuses, a new policy is required. What follows is a sample policy only and does not constitute and is not a substitute for consultation with legal counsel. The law in this area constantly changes and must be reviewed before implementing any policy in this regard. The following sample policy should not be implemented or executed except on the advice of counsel.

Sample Policy

The Firm maintains a voice mail system, an electronic-mail (email) system, and numerous Internet-connected terminals to assist in the conduct of business within the Firm. These systems, including the equipment and the data stored in the system, are and remain at all times the property of the Firm, whether they are located in your home, at a remote location, or in the office. As such, all messages created, sent, received or stored in the system as well as all information and materials downloaded into Firm computers are and remain the property of the Firm. Messages must be limited to the conduct of business at the Firm. Voice mail, electronic mail, and the Internet may not be used for the conduct of personal business. Employee use of the Internet for reasons unrelated to the Firm's business is a violation of this policy unless approved in writing by an authorized manager. The Internet may only be accessed from one of the designated Internet access terminals at the Firm.

The Firm reserves the right to retrieve and review any message composed, sent, received, or downloaded. (Please note that even when a message is deleted or read, it is still possible to recreate the message; therefore, ultimate privacy of messages cannot be ensured to anyone.) Further, the Firm reserves the right to

monitor, at any time, your Internet usage including the Web sites that you have accessed, and any information that you may have downloaded. (While voice mail, electronic mail, and Internet may accommodate the use of passwords for security, confidentiality cannot be guaranteed.)

Someone may review messages and downloaded data other than the intended recipient. Moreover, all passwords must be made known to the Firm. (The reason for this is simple: your system may need to be accessed by the Firm when you are absent.)

Messages and downloaded data may not contain content that may reasonably be considered offensive or disruptive to any employee. Offensive content would include, but would not be limited to, sexual comments or images, racial slurs, gender-specific comments or any comments that would offend someone on the basis of his or her age, sexual orientation, religious or political beliefs, national origin, or disability.

Employees learning of any misuse of the voice mail or electronic mail system or the Internet or violations of this policy shall notify the Firm HR Director, Office Managing Partner or other member of management immediately.

Sample Telecommuting Agreement

I have read and understand the attached Management Telecommuting Policy, and agree to the duties, obligations, responsibilities and conditions for telecommuters described in that document.

I agree that, among other things, I am responsible for establishing specific Telecommuting work hours, furnishing and maintaining my remote work space in a safe manner, employing appropriate Telecommuting security measures and protecting firm assets, information, trade secrets, and systems. I also understand and have completed Exhibit A, which is attached and specifies detailed requirements and rules related to my specific telecommuting situation.

I understand that Telecommuting is voluntary and I may stop Telecommuting at any time. I also understand that the firm may at any time change any or all of the conditions under which I am permitted to telecommute, or withdraw permission to telecommute.

For the Firm

Employee

Date

Telecommuting Security Policy Checklist

Consider the following questions and use them to structure your telecommuting security policy.

Policy and Guidelines

- Does a remote access security policy exist?
- Is the security policy frequently reviewed and revised to reflect technology changes, outmoded approaches, or practice areas or service offerings affecting firm/client relationships and system interaction?
- Does the remote access policy specify guidelines for the selection and implementation mechanisms that control access between authorized users and firm computer and networks?
- Does the remote access policy conform to all existing firm communications guidelines?
- Does the remote access policy address the physical protection of the communications medium, devices, computers and data storage at the remote site?
- Does the security policy require the classification of the functions, applications and data to determine the levels of security needed to protect the asset?
- Does a policy exist to obtain access to important proprietary information at remote sites?
- Does a policy exist which defines who is responsible in case of theft of hardware, software or data at remote sites?
- Does a policy exist for reporting unauthorized activity?
- Does a policy exist for "appropriate" personal use of firm equipment?
- Do remote access users have to sign a form stating they know and understand the remote access policies?
- Is there a formal, complete and tested disaster recovery plan in place for the remote sites?

Identification & Authorization

- Do the remote access security controls require that users be identified before the requested actions are initiated?
- Does each user have a unique identifier (user ID)?
- Does the firm site maintain and use authentication data for verifying the identity of a user?
- Can the security controls uniquely identify each remote access user, device and port?
- Are there automatic time-out or lock-screen capabilities on the remote site equipment to control access during periods of non-use?

Access Control

- Do the remote access security controls limit the unauthorized sharing of users' access rights?
- Does the access control mechanism support the customizing of privileges for each user ID at remote sites?
- Do the remote access security controls protect audit records from unauthorized access?
- Are users provided with last log-in session information?
- Are banners displayed regarding unauthorized usage?
- Are banners displayed regarding the usage of monitoring policy?
- Does the remote site have the capability to encrypt sensitive information including authentication information?
- Are users allowed only one remote connection to the firm network (per user ID or address)?

Auditing

- Does the remote access security mechanism record alarms and authentication violations as a default?
- Does the audit record for each recorded event identify:

- Date and time of the event?
- User or entity?
- Origin of the event (e.g., network address, originating phone number)?
- Type of event?
- Success or failure of the event?
- Is the audit trail information retained long enough to support reviews and analysis by security personnel and to meet firm policy?
- If dial-up access to the remote site is possible, does the audit mechanism record the details associated with each user access?
- Can the security controls uniquely identify each remote access user, device and port?

Integrity

- Are there virus-scanning capabilities required on remote sites?
- How often are they updated?
- Is access to public bulletin boards allowed?
- Are there capabilities to perform network and server congestion management in terms of monitoring, detection and enforcement functions?
- Are measures in place to ensure the proper disposal of confidential data (paper, fax, digital, etc.) at remote sites?

Physical Security

- Are the remote sites in physically secure locations?
- If equipment is stolen, can the perpetrator access proprietary information?
- Is a full physical inventory of remote site equipment and user systems maintained and periodically verified?
- Are backup tapes and media available and secured on-site for remote site equipment?

- Does a policy exist addressing fire, smoke, water and hazardous material contamination damage at a remote site?
- Is all paper data (proprietary, confidential, etc.) physically secure at the remote site?
- Is all computer data (floppies, hard drives, etc.) physically secure at the remote site?
- Is all media destruction (proprietary, confidential, etc.) at the remote site consistent with firm security policies?
- Is there a process for return of equipment and proprietary data upon termination of employment or necessary firm access?
- Does a policy exist for repair of equipment that contains proprietary information?
- Is there insurance for liability and personal injury at the remote site?

Security Administration

- Are organizational responsibilities for remote access security defined?
- Is there a remote access security administrator?
- Is security a part of the defined responsibilities for the personnel who monitor, maintain and control various remote site equipment?
- Is there a process for authorizing new remote users, authorizing and updating remote user access capabilities, and deleting access when no longer needed?
- Are there periodic reviews of remote user privileges to ensure that capabilities remain commensurate with job functions?
- Do security event triggers generate alarms to provide administrator notification?
- Are security alarms properly categorized in terms of severity?
- Are the triggers modifiable by the administrator?
- Do the remote access security controls permit only authorized users (administrators) to grant access privileges to remote site equipment for new, authorized users?

- Do the remote access security controls allow network devices to be isolated when there is a compromise?
- Are there defined administrator responsibilities to isolate a compromised device?
- Do the remote access security controls include test, detecting and reporting communication errors (e. g., high retransmission rate)?
- Is there a way to prevent bypass of the audit and alarm mechanisms by resetting remote access devices to invoke an insecure default configuration?
- Is periodic testing for unauthorized access, denial of service or other security weaknesses performed?
- Is there a defined practice of reviewing audit information on a periodic basis?
- Are there reporting capabilities to provide information on user profiles and access rules?

Security Administration (Cont.)

- Are there adequate controls to restrict access to and use of network troubleshooting equipment (e.g., protocol analyzer)?
- Are there adequate controls to restrict access to and the use of network management software tools?
- Is there a capability to force reauthentication after the server has been unavailable?
- Is there a capability to force sign-off and prevent sign-on during system maintenance?
- Is there the means to run scheduled unattended backups of the remote site equipment?
- Are all security functions and software changes made only by an authorized administrator?

- Is there a way to ensure that only authorized legally acquired software (e.g., applications, and tools) are installed and used on remote site equipment?
- Are backup copies of authorized software and documentation available?
- Are purchasing records and other proof of licensing requirements for software properly maintained? Architecture and Topology
- Is there network equipment in place that can separate traffic according to user communities?
- Is the remote access equipment interconnected with less trusted or untrusted (e.g., Internet) networks?
- In a multiple remote site environment, are all sites maintained at the same security level?
- Are the remote access physical topology and network maps documented, verified and kept up to date?

Education/Awareness/Enforcement

- Are users aware of the signs of a virus or worm?
- Are users familiar with the use of virus scanners?
- Are users aware of the dangers of software engineering?
- Are users aware of the remote access security policies?
- Do remote access users and their managers receive security training prior to using remote access?
- Do remote access users and their managers receive annual security training?

Modem Access

- Is there a single point of entry into the network, i.e., modem pool or terminal server?
- Are all modem phone numbers unlisted?
- Is dial-out allowed at the firm site?

- Do modems exist on individual firm site systems?
- Is auto-answer on dial-in access allowed at remote sites?

The approaches, principles and ideas expressed in this Checklist are merely recommendations to assist the reader and the reader's organization in establishing plans for dealing with information security. This Checklist is not a statement of rules or regulations, nor will following it ensure compliance with any federal, state or local codes or regulations. Specific issues should be addressed to the appropriate federal, state, local agency, or risk management personnel.

Other Resources

In creating this guide, we have attempted to collect in one document a number of topics pertaining to Telecommuting in order to present as complete an overview as possible for both Teleworkers and Firm Decision-makers.

There are a number of resources available that address many of these topics in more depth and detail. A partial list is as follows:

Books

- 101 Home Office Success Secrets - Lisa Kanarek. Hawthorne: Career Press, 1994
- Home Offices & Workspaces - Sunset Books & Magazines. Menlo Park: Sunset, 1991.
- Making Telecommuting Happen, A Guide for Telemanagers and Telecommuters - Jack M. Niles. New York: Van Nostrand Reinhold, 1994
- Managing the Home Based Worker - Philip E Mahfood. Chicago: Probus. 1992
- Teleworker Guidebook, There's No Space Like Home - Charlotte Damato. Scottsdale: Marshall-Qualtec. 1997.
- The Joy of Working from Home - Jeff Berner. San Francisco: Berrett-Koehler, 1994.
- The Telecommuter's Advisor - June Langhoff. San Francisco: Aegis, 1996
- The-Work-At-Home Sourcebook - Lynie Arden. Boulder: Live Oak, 1994
- Working Smarter from Home - Nancy Struck. Menlo Park: Crisp, 1995.

Articles

- Kiss the Office Goodbye! PC World - October, 1994. Pp. 143-145, 150, 155-157.
- Telecommuting Boosts Employee Output. HR Magazine - February, 1994. Pp.51-53

- Telecommuting Tips. PC World - December, 1995. Pp. 170-178

Studies & Surveys

- Smart Valley, Inc. ® Telecommuting Pilot Results. Gemini Consulting & Smart Valley, Inc. ® Telecommuting Project. October, 1994 *
- Telecommuting, Two Years Later. Strategic Decisions Group for Smart Valley Telecommuting Project. February, 1996*
- Telecommuting – 1997. Decisive Technology for Smart Valley Telecommuting Project. November, 1997* * Available only on the World Wide Web at: <http://www.svi.org/telework>