# Teleworking Policy and Procedures

## Policy Overview

Teleworking & telecommuting is also called "remote work", “work from home”, or "telework". It is effectively somebody who telecommutes or works from home or another location other than the main office or facility where they traditionally work. With advances in technology, individuals are teleworking & telecommuting more than ever before, which ultimately requires that comprehensive policies, procedures, and processes be in place for such initiatives.

### Teleworking & Telecommuting Rights

Teleworking & telecommuting, herein referred to in this policy and procedures document, is a privilege granted to employees for helping promote efficiencies in the workplace, while still maintaining quality and consistency with one’s work roles and responsibilities. Teleworking is a work place environment protocol that is fully embraced by [company name] because many employees can increase productivity with teleworking, and often employees require such flexibility as traditional working hours and places of business are not conducive. Teleworking thus means to work from the employee’s home or from an office near the employee’s home, rather than from the main place of employment.

Teleworking is not for everyone, and is not deemed to be a reward for work performance, rather, a useful platform for which users can continue to perform their daily roles and responsibilities. For any employee to be considered for teleworking, authorized personnel at [company name] are to assess the impact of teleworking in regards to an employee’s overall productivity. Specifically, this means taking in to account an employee’s job functions, such as the ability for teleworking to continue to allow such job functions to be performed at optimal levels, the ability to effectively communicate with an employee, the prospects of an employee continuing to grow and learn as necessary, along with other factors deemed important for [company name].

### Physical Security Environment

While [company name] will not confine an employee to a specific teleworking location, it is critical that for each location to be used, adequate physical security controls are to be in place for protecting both the employee and all relevant assets (i.e., computer, etc.) used while teleworking. Best practices measures relating to physical security are to consist of the following:

- Working in areas that allow employees an adequate degree of privacy from other individuals, such that no eavesdropping or any other type of malicious social engineering tactics can be initiated.
- Ensuring that employees can safely exit and escape in a reasonable timeframe from any physical and or environmental threat posed.
- Ensuring the appropriate access controls are in place for securing the teleworking environment, such as traditional lock and key, punch code, electronic access control system, etc.
- Ensuring that appropriate heating, ventilation, and air-conditioning (HVAC) elements are in place.
- If necessary, and due to the sensitivity to the work being performed at the teleworking environment, appropriate security and monitoring controls are to be in place. Thus, "security" and "monitoring" implies that the facility has in place the following physical security and environmental security controls:
    - Constructed in a manner allowing for adequate protection of the teleworking environment.
    - Security alarms that are active during non-business hours, with alarm notifications directly answered by a third-party security service or local police force.
    - The use of cages, cabinets, or other designated, secured areas for securing the specified information system.

- Access control mechanisms consisting of traditional lock and key, and/or electronic access control systems (ACS), such as badge readers and biometric recognition (i.e., iris, palm, and fingerprint scanners/readers). Furthermore, all electronic access control mechanisms are to record all activity and produce log reports that are retained for a minimum of [x] days.
- Adequate closed-circuit monitoring, video surveillance as needed, both internally and externally, with all video kept for a minimum of [x] days for purposes of meeting security best practices and various regulatory requirements.
- Appropriate fire detection and suppression elements, along with fire extinguishers placed in mission critical areas.
- Appropriate power protection devices for ensuring a continued, balanced load of power to the specified information systems, thus mitigating power surges and spikes.

- [Company name] personnel have the right to inspect one's teleworking environment as necessary, yet will provide reasonable notice.
- Upon inspection, [company name] reserves the right to make any necessary changes to the teleworking environment.
- The teleworking environment is to adhere to all necessary physical security and environmental security requirements as mandated by applicable laws, regulations, client and contractual requirement, etc.

**Communications and Information Security Requirements**

Some of the best practices to use for ensuring the CIA triad of Confidentiality, Integrity, and Availability is upheld at all times is Defense-in-Depth and Layered security - essentially utilizing various resources for helping protect one's teleworking environment. Defense-in- Depth – for purposes of information security – includes the following layers, which have been loosely adopted and agreed upon by industry leading vendors and other noted organizations:

- Data
- Application
- Host
- Internal Network
- Perimeter
- Physical
- Policies, Procedures, Awareness

Layered security, often mentioned in the context of Defense-in-Depth, is a concept whereby multiple layers of security initiatives are deployed for the purposes of protecting an organization's critical information systems, such as one's teleworking environment. Specifically, by utilizing a number of security tools, protocols, and features, organizations can effectively put in place layers of security that – in the aggregate – help ensure the confidentiality, integrity, and availability (CIA) of systems. As such, employees that telework are to ensure that all communications and information security requirements for teleworking have adopted the concepts of Defense-in-Depth, and Layered Security.

**Remote Access**

Remote access is often necessary for an employee to perform his/her respective job functions, and as such, the following initiatives are to be in place:

- The [company name] remote access platform is to consist of communication protocols, and other supporting devices the ultimately ensure the confidentiality, integrity, and availability of such connections, along with the organization's network.

- The use of remote access is a privilege - one that is to be assigned only to authorized individuals with a justified business need for such access - and only after comprehensive analysis and subsequent approval procedures have been undertaken by applicable supervisory personnel and all necessary I.T. authorities.

- Unique usernames and passwords that meet or exceed stated best practices for complexity rules are to be implemented for all users with remote access rights. Also, stated lockout times for idle remote access sessions, along with predefined time parameters (i.e., 180 minutes, etc.) for allowing such access rights are to be configured accordingly.

- Two-factor authentication, which requires use of two (2) of the following three (3) methods of access – something you know, something you have, something you are – is to be incorporated as necessary for compliance purposes, specifically for that of PCI DSS compliance, HIPAA, and many other legislative mandates and industry specific directives.

- It is the responsibility of [company name] I.T. personnel to ensure that all information systems that facilitate and administer remote access rights are current with all applicable security upgrades and patches.

- Should a user suspect or confirm that an actual security issue has arisen relating to one's remote access session, the user is to terminate the remote access session and report the incident immediately to authorized I.T. personnel.

- Remote access is a privilege; thus, all authorized users are to utilize such services for business use only, with no personal or questionable activities allowed. "Business use only" implies the following: (1). for facilitating all required duties for a stated job function, (2). for communicating with other authorized parties (i.e., employees, clients, contractors, etc.), (3). for conducting research applicable to one's job duties.

- [Company name] reserves the right to monitor one's remote access sessions without consent, which may include installing agent software on end-user systems for a variety of security, performance, and overall monitoring issues.

- Personal and confidential information is never allowed to be stored on any local devices used for enabling a remote session, such as one's hard drive, or using external storage devices via USB connections.

**Remote Access Security Measures**

Because of the different types of remote access mediums and protocols allowed, along with the numerous devices that can be used for initiating remote access sessions, the following security measures apply:

- Remote access client software – if residing on a user's device – is not to be altered in any way.
- Personal firewall software must be enabled on computers, along with other malware protection measures, such as a current, known, and stable version of anti-virus.
- Along with not altering remote access client software, users are also forbidden from altering and changing any configurations on [company name] information systems that would affect the security of such systems, and also the remote access session.
- Users are forbidden from initiating remote access sessions from untrusted end-user devices that are not owned, operated, maintained, and controlled by [company name] and pose a serious security threat. Common examples include the following: mall kiosks that offer Internet services, hotel business |

computer rooms offering PC's for use, office supply | mailing stores providing computers for printing, faxing, scanning services, etc.

- Users are forbidden from engaging in dual connectivity | concurrent connectivity, whereby a user is connected to the [company name] network, while also on another network.
- Remote access rights are strictly for authorized users who have been assigned such rights, and not for any other individuals, such as personal friends, family members, co-workers, etc.
- Confirmation of remote session termination, such as closing out of the program and the browser, is to be conducted after each session. As a security precaution, [company name] has implemented a pre-determined "time-out" clause for remote access for helping increase security.

In summary, the same consideration that is given to a user's onsite connection to the [company name] network must also be utilized for remote access sessions. Additionally, users are to display reasonable and prudent security measures for ensuring the physical safety of any [company name] devices for establishing remote access sessions. This would include not leaving laptops in untrusted environments, safely securing devices when in public domains, etc.

**Security Parameters for Unauthorized Access**

Only authorized personnel are to access the teleworking environment; thus, family, friends, and other relevant personnel are to be restricted from gaining access to such facilities. While many teleworking environments outside of an employee's home are that of shared office space, please ensure that all teleworking equipment is thus secured at all times. When at home, please ensure best practices are in place for ensuring unauthorized access is not allowed, thus locking doors and securing teleworking equipment when not in use is.

**Home Networks**

Employees that telework perform job functions that require them to store, process, and transmit sensitive and confidential company information over their personal networks, which can pose significant security risks. As such, the following initiatives are to be in place for securing an employee's home network.

- **Use Anti-Virus.** Whatever computer you are using on your home network, it must have current, updated anti-virus on it. This is one of the most fundamentally important - and easy to implement - security safeguards as it protects your computer from malware and other malicious exploits.

- **Use Strong Passwords.** Whatever you are doing online, it's a good idea to use very strong passwords, those that contain a mixture of letters, numbers, and symbols. This applies to your actual computer for which you're logging onto. Remember, home means "home", where children and spouses have access to your items, so protecting them from misuse is important.

- **Use a Personal Firewall.** A personal firewall is an extra layer of added protection for helping protect your home network in the following manner:
  - Protects the user from unwanted incoming connection attempts, ultimately allowing the user to control which programs can and cannot access the Internet.
  - Blocks and/or alerts a user about outgoing connection attempts.
  - Monitors and regulates all incoming and outgoing Internet users.

  There are a number of commercially developed software programs you can install to act as a personal firewall, yet you can also use the Windows personal firewalls software from Microsoft, which is highly effective. As for Apple, their Mac books also have a built-in personal firewall option, which should also be used.

- **Be Cautious Online.** Remember that working from home means you're accessing [company name] information, so be smart about what websites you're visiting, information you are downloading, etc. Being cautious and having a "security first" mindset is a must at all times.

- **Change your WI-FI broadcast**. Known technically as an SSID, it's the wireless (if you are in fact using wireless) network you connect to. Make sure to change the default SSID to something more unique. SSID's that are left with their default names often are an indicator to hackers that the passwords are also still the same default that was shipped with the devices. Thus, change both the default SSID and the default password. Your router is the bridge to the Internet, so protect it by removing many of the default settings.

- **Enable MAC filtering.** Additionally, you want to allow wireless access only to trusted laptops, by allowing wireless connections only to known MAC address. MAC (Media Access Control) address is a unique identifier attached to most network adapters - which, in this case - would be the unique identifier of your laptop wireless adapter.

- **Change Default Wireless Access to your Router.** The default password for wireless web access is essentially the same for the specified model of a wireless router assigned by the manufacturer, thus it's important to change default password of the wireless router web access immediately.

**Intellectual Property**

Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce. Therefore, [company name] IP is protected in law by patents, copyright and trademarks, which enable [company name] to earn recognition or financial benefit from what they invent or create. **Source:** http://www.wipo.int/portal/en/.

As such, any [company name] IP accessed, used, and developed on non-company information systems (i.e., privately owned information systems) is fully owned and controlled by [company name]. Furthermore, for additional information on IP, please contact authorized personnel within [company name].

**Access to Equipment**

At any time, with or without notice, [company name] has the right to access any information systems and other supporting devices (i.e., equipment) being used by an employee while teleworking for [company name]. While the nature for accessing such equipment is largely for preventative maintenance and security patching, other reasons may also be warranted. As such, employees are to provide full cooperation and access to equipment as needed by authorized personnel within [company name].

**Software Licensing Agreements**

Employees engaged in teleworking activities are to abide by the following software guidelines, responsibilities, and acceptable use:

- All software is to be configured and used strictly for business operations.

- All software is to be appropriately hardened and secured in accordance with industry standards and for applicable business requirements. Appropriate hardening procedures and guidelines may be obtained from any number of industry resources.

- If software is developed internally, all development of software must be appropriately hardened and secured in accordance with **The Open Web Application Security Project (OWASP),** http://www.owasp.org

- Software vendors provide alert boards, security forums, white papers, and other additional sources for hardening and securing software as needed. Please check with your software vendor in ascertaining this information, if necessary.

- All users are responsible for understanding and adhering to all applicable licensing rights and agreements pertaining to [company name] software resources.

- All software obtained for licensing rights by [company name] will be viewed as property of [company name], with no rights of ownership afforded to users under any circumstances.

- All software developed internally by [company name] will be viewed as property of [company name], with no rights of ownership afforded to users under any circumstances. This includes, but is not limited to, the following: (1). Software source code (2). Software escrow agreements. (3). All other software resources (change tickets, software residing in test or staging environments, etc.) related to [company name] internally developed software.

- Any software obtained without proof of purchase and licensing rights will not be allowed onto the network.

- All users must be responsible for the proper use of software resources, which entails using these resources in a professional and ethical manner at all times.

- All users and their subsequent activities undertaken on software resources are subject to audit and review as needed.

- Violations and penalties for illegal use of software resources are punishable by fines and imprisonment. The financial amount and imprisonment sentence, if any, will be determined by designated authorities and a court of law.

- Users are to have their access rights permanently revoked from all computing systems that allow for access to any software resources once they have been terminated.

Additionally, [company name] also has a documented Software Usage Policy and Procedure that provides additional information regarding the use of software and related licensing.

**Malware Protection and Network Security Requirements**

Anti-virus and anti-malware solutions utilized by [company name] employees that telework must be from an approved vendor, one that offers ongoing customer support pertaining to the installation and maintenance of the applicable software. Specifically, this includes all necessary installation documentation (i.e., manuals, user administrator and setup guides, hardening guides, etc.), "virus support" initiatives, such as providing updates for new detection signatures and the applicable dictionaries, etc. Simply stated, whatever computer an employee is using for teleworking, it needs to have current, updated anti-virus on it. This is one of the most fundamentally important - and easy to implement - security safeguards as it protects your computer from malware and other malicious exploits.

Additionally, a personal firewall is to be used as this provides an additional layer for helping protect a teleworking employee's home network in the following manner: (1). Protects the user from unwanted incoming connection attempts, ultimately allowing the user to control which programs can and cannot access the Internet. (2). Blocks

and/or alerts a user about outgoing connection attempts. (3). Monitors and regulates all incoming and outgoing Internet users.

**Type of Work Permitted**

Activities performed by employees that are teleworking are to be strictly associated with their respective job functions, roles and responsibilities such employees have been assigned to. While [company name] understands that personal activities do occur during work related hours – such as answering personal emails, taking personal calls, etc. – employees are nonetheless to spend their time performing work related duties as their primary function.

During defined teleworking hours, which is to consist of normal business hours as described by [company name] human resources, employees are to have access to whichever internal systems at [company name] are needed to perform their work-related duties. When connecting to internal systems at [company name], only approved protocols are to be used for ensuring the confidentiality, integrity, and availability (CIA) of the remote access session.

**Suitable Equipment**

All equipment used by employees teleworking must be approved by authorized personnel at [company name] for ensuring it is both appropriate and sufficient for work use. Equipment can include all types of information systems and other supporting devices necessary for one to perform their respective job duties. Non-approved equipment, regardless of how safe, secure, or efficient such systems may be, are not to be used at any time by teleworking employees.

Furthermore, equipment is allowed to be inspected at any timey by authorized personnel at [company name], and users are not allowed to modify and/or disable any configurations on equipment without prior approval. All equipment owned by [company name] is to be returned in good working order if an employee is no longer teleworking, or that employee has been voluntarily or involuntarily terminated from [company name].

**Family and Visitor Access**

Only authorized personnel are to be allowed to access the actual space for which a [company name] employee is teleworking. Because many employees will be teleworking from home, it is important to work in an area that is safe and secure in that only an employee can physically access the designated area during normal business hours. Once such normal business hours are over, then all teleworking equipment is to be secured as necessary, especially if the area then becomes a place where friends and family members may visit. As for teleworking at other locations other than one's home, [company name] employees are to use their discretion and best judgement regarding who can access the facility being used and in what capacity.

**Hardware and Software Support and Maintenance**

All equipment used by [company name] employees while teleworking is to maintain up-to-date hardware and software as necessary. For hardware, this means using approved equipment that allows employees to work securely and efficiently. For software, this means ensuring that equipment has current patches and security updates installed, along with license agreements allowing the use of such software on equipment.

Additionally, at any time, [company name] authorized personnel are to be able to access all hardware and software for performing necessary support and maintenance activities for ensuring the safety and security of such equipment.

**Insurance**

Appropriate insurance is to be maintained for all teleworking equipment used by employees of [company name]. The legal department within [company name] maintains all information pertaining to insurance coverage, therefore, any questions regarding insurance for teleworking equipment is to be addressed to such personnel as needed.

**Backups and Business Continuity**

While teleworking, [company name] employees are to save information while connected to the network, thereby allowing such data to be ultimately saved with the backup process being performed by authorized I.T. personnel.

Employees are forbidden from saving information on equipment (i.e., desktops, laptops, etc.), as such devices could be easily destroyed during a disaster.

[Company name] employees that are teleworking are to also ensure that adequate Business Continuity and Disaster Recovery (BCDRP) initiatives are in place for ensuring the safety and security of individuals, along with the ability to continue operations in the event of a disaster. [Company name] has in place a documented BCDRP plan, for which all employees have been provided a copy as necessary. As for employees that are teleworking, each employee is to provide an assessment of the physical location for which they are teleworking, and what BCDRP initiatives are in place. This process is to include communication with authorized personnel at [company name] for ensuring such a plan is acceptable and documented.

### Audit and Security Monitoring

At any time, [company name] may employ all necessary audit and security monitoring tools and techniques for helping ensure the safety and security of data and information being accessed at the teleworking environment for which employees are located. Common audit and security monitoring initiatives include the following:

- **Configuration and Change Monitoring:** The use of specialized software, such as File Integrity Monitoring (FIM), Host based Intrusion Detection Systems (HIDS), and/or change detection software programs are to be implemented for monitoring servers as they provide the necessary capabilities for assisting in the capture of necessary events. Additionally, configuration change monitoring tools are to be used to detect any file changes made within a specified information system, ranging from changes to commonly accessed files and folders, to more granular based data, such as configuration files, executables, rules, and permissions.
- **Performance and Utilization Monitoring:** Additional measures are to be employed for ensuring that information systems are actively being monitored for all necessary performance and utilization measures, such as the following: (1). CPU Utilization. (2). Memory Utilization. (3). Disk Utilization.

### Revocation of Teleworking & Telecommuting Rights

At any time, [company name] has the right to implement revocation procedures regarding teleworking for any employee. Any number of factors could lead to such rights being revoked, ranging from performance and security issues to operational and financial constraints. When such measures are put in place, [company name] employees are to assist authorized personal as necessary.