



## How to Implement a Successful Telecommuting Program

---

## Introduction

---

This white paper is intended for companies and CIOs with an existing telecommuter program or those wanting to launch such a program. We will highlight current practices and trends, implementation considerations, and technical options. The idea of telecommuting has gained significant momentum due to increasing pressure on companies to cut costs and increase employee productivity. Companies are now challenged to redefine the idea of corporate offices. The expansion of broadband services to employees' homes has made telecommuting a viable option—and sometimes a requirement—for today's medium to large-sized businesses.

The benefits of expanding access beyond the corporate walls are compelling and include:

- Reduction in operating expenses
- Improved employee work-life balance
- Increased employee productivity
- Increased quality contact with customers
- Reduced company carbon footprint

Some typical telecommuter activities include:

- Customer/technical support employees tapping into corporate computing resources to perform troubleshooting tasks
- Managers connecting after hours to catch up on email
- Remote/traveling employees connecting to the corporate office
- Employees who participate in “flex time” programs, which permit several telecommuting hours per week

The popularity of telecommuting and remote access programs has surged recently due to the following drivers:

- Initiatives to reduce corporate costs and improve employee productivity
- Advances in low-cost, high-performance access technologies—such as xDSL and DOCSIS cable
- Improvements in information security—such as VPNs, digital certificates, firewalls, and data encryption algorithms
- Convergence of voice, video, and data on a common IP framework

---

## Background

---

Until recently, companies wanting to provide telecommuting capabilities to their employees were constrained at the “last mile” access point. Their choices were either slow-and-difficult-to-support dial-up modem access, or slow-and-expensive-to-install frame relay or dedicated access circuits. The cost and speed limitations of these access methods made full-scale telecommuting a challenging proposition.

In the past few years, DSL and cable-based broadband technology has matured dramatically. Managed services providers (MSPs) have electronically bonded their provisioning systems directly with the RBOC, ILEC, and DLEC internal systems, so prequalification is more accurate and installation is more streamlined. Cable companies have brought business class cable modem service to market and have interconnected their last mile service into fiber optic backbones for improved speed and reliability. Some of the more forward-thinking providers offer service level agreement (SLA) commitments to their business customers to address uptime, performance, and repair.

A number of emerging market and technology trends have inspired CIOs to replace their decentralized, unmanaged approach to telecommuting with a formal, well-defined policy and technology set. CIOs have been forced to lock down and centralize all access into the corporate network due to the ever-increasing threat of viruses and security attacks. By publishing a formal telecommuting policy with strict rules for accessing the corporate network, many of these threats can be avoided or dramatically diminished. Laptops running encrypted VPN software with automatically updated virus protection and personal firewalls are a practical way to provide the easy access employees require while maintaining centralized management, control, audit trails, and security.

## Implementation Considerations

### Success Factors

There are a number of success factors to consider when deploying a telecommuting program. Critical technology issues—such as security, access, asset management, reliability, and support—are vital. “Softer” considerations—such as ensuring employee fairness, as well as maintaining workplace culture, corporate legal protection, and trust—also must be considered. Successful telecommuting programs require thorough communication, corporate support, technology standardization, well-defined processes, ongoing training, and robust implementation tools. A telecommuting program that is well planned, implemented, and managed is an effective work option.

After the program policies and scope are established, a large number of technology issues must be addressed:

- Plan and execute seamless integration with the existing corporate network
- Select, test, stage, configure, and deploy standardized, scalable, and supportable equipment
- Choose appropriate access partners to provide safe and reliable network connectivity
- Make decisions regarding information security and public vs. private transport
- Define user enrollment, installation, provisioning, and support processes
- Make, test, standardize, and deploy decisions about firewall configurations, data encryption ciphers, routing protocols, VPN types, and hardware/software interoperability

The most challenging technical telecommuting hurdle is multi-vendor integration. A daunting number of vendors and access technologies must seamlessly interoperate in order to provide secure, reliable remote access to corporate computing resources. The following are the major milestones and possible fail points:

- Integrate customer premise equipment (CPE), network equipment, VPN hardware and software, firewalls, operating systems, as well as telco providers and their corresponding release updates, software patches, bug fixes, and firmware upgrades
- Evaluate and test remote or mobile user software applications for performance over various connectivity and security methods
- Analyze the technology outsourcing strategy to determine whether it would be better supported internally or if an outsourced vendor with telecommuting and VPN expertise would be a better option

---

## How to Begin

---

Implementing a successful telecommuting program requires much more than simply providing a high-speed connection and a laptop. There is an enormous amount of planning that must take place to accommodate policies and procedures, technology selection, training, installation, technical support, cost and budget management, and ensure user satisfaction.

Begin by carefully planning and documenting the key phases of the project. Build a policies and procedures manual that includes:

- Selection criteria for participation
- Participation requirements and enrollment procedures
- Telecommuter agreement and contract
- Office supply policy
- Home office setup guide
- Administrative support policy
- Mail and overnight package procedures
- Program termination policy
- Training program outline (technology usage, time management, decentralized meetings, cultural issues, etc.)
- Accounting and expense submission/reimbursement policy
- Technical equipment and policies

---

## Planning

---

Detailed technical and operational planning is critical to the success of any telecommuter program. Poor planning can result in frustrated users and could compromise business computing resources. The technology bundle that telecommuters will use to work remotely includes hardware—such as computers, phones, modems and printers—and software—such as operating systems, applications, firewalls, security keys, backup software and diagnosis tools. The heart of the telecommuting technology bundle is the virtual private network (VPN). The VPN is comprised of the hardware and software required to gain authorized access to the corporate network. It can include security tokens, phonebook/dialer software, hardware or software-based data encryption, shared authentication keys, and preconfigured tunnel paths to authorization servers. Careful consideration must be given to plotting out security, designing access methods, establishing hardware and software standards, and planning for ongoing upgrades/patches/bug fixes. Companies may seek outsourced vendors and technology partners to assist with the planning, deployment, and operation of the project. Select a partner that has a track record of implementing a successful telecommuting program and has outlined best practices procedures to help navigate the myriad of challenges.

Telecommuting technologies are largely transparent to the user, so the ultimate gauge of each telecommuter's satisfaction is the user experience. Plan for a single, integrated VPN and dialer graphical user interface (GUI) that makes establishing a secure connection seamless. Be sure the front end is smart enough to present the same look and feel, regardless of access method. The technology should also include the firewall, digital certificate, virus protection, and other embedded software in the background, so the telecommuter does not have to manually launch or configure each aspect individually.

It is difficult to balance supportability and standardization with the economics of leveraging existing equipment. Some sample considerations include:

- Issuing new preconfigured PCs for maximum standardization and minimum support costs vs. reloading existing PCs with new VPN and application software to minimize capital expenditures (capex)
- Distributing VPN and application software on CDs or via email for telecommuters to self-install vs. having the IS or help desk staff install all of the software

Successful planning will make provisions to accommodate all of these situations and work to find the proper balance between standardization, control, user satisfaction, and budget.

---

## Implementation & Deployment

---

The most difficult task of any telecommuting initiative is implementing and deploying the solution to the workforce. Typically, one of the most difficult processes is selecting and ordering the appropriate access connection for each telecommuter and then managing the installation. After ensuring that the telecommuter candidate is approved for the program, the next step involves assessing which technologies are available in the user's geography, which of technologies can reach the telecommuter's home, and what bandwidth options are available. Most companies will probably select a DSL or cable modem service because of the attractive speed/price offer. However, the actual ordering and installation of the service can be time consuming.

Typically, finding the right access method involves researching each phone company, cable company, or telecommunications provider in each telecommuter's coverage area to determine service availability. It becomes quickly apparent that there is not a single source broadband provider that can reach all of the telecommuter locations. The task of matching service providers to telecommuter area and then managing the ordering and installation processes can quickly become an unwieldy multi-vendor challenge.

Once the telecommuter is prequalified for the appropriate access type/speed, the next challenge is to coordinate the installation and track its progress—installation dates, circuit installation dates, hardware configuration and setup, and inside wiring. Some VPN service providers have developed web-based implementation tools to greatly ease the broadband access “pre-qualification”, installation management, and activation processes.

---

## Maintenance

---

Supporting and maintaining a group of telecommuters—even with the best training and planning—can be difficult. Questions which would normally arise in the office and would probably be handled by asking a coworker are now the sole responsibility of technical support. Because telecommuters are usually physically isolated from other workers, their workflow is very dependent upon the proper functioning of their technology bundle and responsive technical support. Studies show that telecommuters tend to work longer hours—usually well into the evening—when most traditional office workers have gone home. CIOs have the challenge of deciding the window of opportunity—limit to normal business hours or extend the hours—for technical support. Most telecommuters prefer a centralized, single point of contact support model that enables telecommuters to articulate the problem once to a sole contact, who then either remedies the issue or draws from additional resources.

A hardware failure can cause the telecommuter's workflow to come to a complete standstill. To decrease failure-related downtime, consider instituting a mandatory data backup policy and installing automated, unattended backup software on the telecommuter's PC. Also consider keeping a minimum level of “hot spares”—including PCs, cable/DSL modems, routers, VPN appliances, etc.—that are preconfigured and kept on hand for fast shipment to the telecommuter or choose a service provider that offers this type of CPE maintenance. The volume of calls and occasional need to make onsite visits to assist telecommuters has inspired many companies to outsource this function to either their telecommuting service provider or to a technical support company that has remote field agents. Whether you choose to use in-house or outsourced technical support personnel, it is important to implement adequate troubleshooting tools and repair processes to keep telecommuters productive. Technical support experts who are proficient in the following categories should be available to your teleworkers:

- Hardware repair
- Application software support
- Telecom and network support
- Provisioning
- Installations/software removal

In addition, providing a well-defined escalation path within the in-house IT department and outsourced partners is essential for a seamless customer service experience.

In addition to reactive support that addresses telecommuter assistance requests, many CIOs are embracing a proactive VPN network management and monitoring philosophy. To minimize outages and telecommuter problems, consider extending WAN management tools to monitor the telecommuter broadband connection endpoints, as well as measure uptime and performance. So VPN endpoints and corresponding SLAs can be monitored, some VPN service providers offer portals into their management systems.

Depending on the complexity of the VPN, there are numerous hardware, software, and firmware components provided by vendors that continually release upgrades, patches, fixes, and enhancements. Each upgrade/patch release must be evaluated and then evaluated within the interoperability context of the technology bundle to ensure that telecommuters will successfully connect to the resources they require. VPN service providers that offer CPE management maintain records of each user's hardware, firmware, and configuration so they can automatically and transparently provide upgrades/patches to end-users.

## Technical Considerations

---

A comprehensive telecommuting program strategy includes a well-planned technical architecture that is evaluated within the context of a company's existing LAN and WAN environment. The goal is to create the optimum technical design that:

- Leverages the existing network infrastructure
- Creates a seamless extension of the LAN to telecommuters
- Minimizes security risks
- Establishes a framework for adding additional services—such as VoIP and video
- Maximizes supportability via use of industry standards

## Network Design

---

One of the first things to consider is types of remote access technology. The choices range from slow and cumbersome dial-up to expensive dedicated private circuits. For most telecommuting programs, however, the best choice is a VPN, which uses fast, inexpensive broadband over the public Internet. This is often supplemented with dial-up VPNs over the public Internet for times when the telecommuter is mobile. Alternatively, for extremely sensitive data, a network provider that offers a private IP environment can be considered. Typically, these providers have interconnected their backbones privately with last mile broadband providers; because of this, they can keep the telecommuting traffic off of the public Internet and on their private links. This is generally more expensive than using data encryption and the public Internet for transport.

For telecommuters, there are two main VPN technology models to choose from, regardless of whether using the public Internet or private transport for connectivity:

- **IP-Security (IPSec)**

A secure, encrypted data path is set up between the user and the host server, typically a VPN concentrator.

- **Secure Socket Layer (SSL)**

Security and encryption are incorporated into the Web browser, such as Microsoft® Internet Explorer or Netscape® Navigator; SSL only provides access to web-enabled applications, such as email or file sharing. Therefore, applications that require client software—such as ERP or CRM systems—are relegated to IPSec VPNs. In recent months some vendors have released “client-based” versions of their SSL VPN offering, in which users launch an application window to run non-web-enabled applications.

In either model, the telecommuter's traffic is encrypted and tunneled to a corporate security device (VPN concentrator), where it is validated and decrypted through the corporate firewall into the corporate network.

For IPSec VPNs, the next decision is to determine how the VPN sessions will originate—with software-based VPN technology or a hardware-based VPN appliance. In the software-based model, only the traffic coming to and from the telecommuter's PC is encrypted in VPN tunnels; with the hardware-based model, all traffic going through the appliance is encrypted.

An important factor is understanding and accommodating other Internet traffic originating the telecommuter's residence. If the telecommuter has other PCs that access the Internet using the broadband connection or lives with another telecommuter who works for a different company, then the best option is to use a software-based VPN that is loaded on the telecommuter's business PC. Even though hardware VPN devices can be configured to only tunnel traffic that originates from specific PCs and user authentication is required to access corporate resources, many companies prefer establishing the VPN session directly from the telecommuter's PC. If firewall or antivirus software is tampered with, the session is disconnected automatically.

## Hardware Requirements

Regardless of which VPN model is chosen, hardware must be considered. In addition to the PC, CPE equipment to terminate the DSL, cable, ISDN, or other broadband connection must be used. In some cases, this is a modem that connects the broadband service to the telecommuter's PC; in other cases, it is a combination of equipment—including a router, hub, wireless access point, firewall, or VPN appliance. Like most large-scale technology deployments, standardization is critical to maintaining adequate support levels.

Driving standardization can become difficult because each DSL or cable provider (BellSouth<sup>®</sup>, Verizon<sup>®</sup>, Cox<sup>®</sup>, Road Runner<sup>®</sup>, etc.) deploys its own broadband network equipment and selects CPE that is compatible with it. From a support perspective, managing all of the different CPE devices and understanding their configuration utilities when setting up filters, firewalls, and access lists, as well as provide upgrades can be a challenging proposition. Moreover, if VPN appliances, wireless access points, or hubs used to connect multiple PCs are deployed, the telecommuter can quickly amass a large stockpile of equipment—complete with patch cords, power supplies, etc.—that could result in an unsafe, unreliable, or overheated environment.

## Options for Internet Access

### Dial-up Access

Although dial-up does not provide much bandwidth; it is widely available and very straightforward. Dial-up can provide centralized network access to the corporate LAN or WAN via internally managed modem banks or RAS servers. However, it can have expensive per-minute charges for users outside the local calling area. Alternately, purchase plans are available from a national dial provider with thousands of local numbers.

### DSL Access

Digital Subscriber Line (DSL) is a proven technology that uses existing telephone lines to provide high-speed bandwidth access. DSL is a distance-sensitive service with speeds relative to endpoint distance from the central office housing the Digital Subscriber Line Access Multiplexer (DSLAM). Not every local phone company's central office has the proper equipment, so the service is not universally accessible. However, DSL is widely available in larger cities.

DSL can provide speeds equal to or better than traditional 1.5 MB T1 services when the telecommuter's home is within a mile of the central office. This speed drops proportionally as distance from the central office increases. Typically, access becomes unavailable beyond 3.4–3.8 miles. There are multiple types of DSL, but the three most common are:

- **Asymmetrical (ADSL)**

- Provides fast download speed and slower upload speed, generally priced below \$100/mo

- **Symmetrical (SDSL)**

Provides equal upload and download speeds

- **Integrated (IDSL)**

Can run greater distances than ADSL or SDSL, but has a maximum speed of 144k

Generally, ADSL is best suited for telecommuters because it is less expensive. SDSL is typically best suited for small offices and multi-user VPNs because it offers higher levels of performance. There are other, far less available forms of DSL—including G.Line, S/HDSL and VDSL—that promise faster speeds and greater distances. These technologies have not yet been embraced by the market and are not generally available.

### **Cable Modem**

In the past few years, cable companies have spent millions of dollars upgrading the high-speed access services to be more “business class.” They laid fiber-optic cable, and optimized routing and network technologies so individual user speeds are no longer negatively impacted by other users.

### **Security**

In addition to IPSec and SSL-based VPN encryption, there are additional security considerations to evaluate when deploying a telecommuter program. Review internal security policies to ensure that they extend to the telecommuting workforce. Realize there are multiple levels of a sound security methodology including physical security, access security, and data security.

### **Value-added Applications**

When deploying a telecommuting program, it is important to plan ahead and attempt to future-proof the investment. Select standards-based technologies and build an open framework to support additional IP services and tools as they become relevant. Consider an inexpensive dial backup strategy for those rare times when the broadband connection is unavailable. This could be an automated “dial failover” that initiates a dial VPN session from the CPE if the primary link goes down; it could also be a simple process of training users to use their manual dial-up VPN capabilities if the broadband becomes unavailable.

Over time, telecommuters will request and use enhancements and productivity tools—such as voice/video/data convergence and unified data communications, as well as instant messaging. CIOs will need to make decisions regarding the safety and security of using these applications. To improve communications with other telecommuters and employees in traditional offices, consider online collaboration tools, web-based “presentation rooms,” and desktop video conferencing. IP Telephony can be an extremely effective means of eliminating long distance phone calls between the telecommuter and headquarters, and extending office PBX functionality to the home. High-speed broadband connections and secured VPNs make webcams and online meetings a viable option. Telecommuters are going to request these value-added applications, so CIOs must think ahead and formulate a technology roadmap. By articulating the plans for improved and expanded services, telecommuters will be less inclined to do it themselves and increase the support burden. Moreover, a well articulated plan will make for more satisfied telecommuters and create volunteers to help pilot new and innovative ideas.

### **Buy vs. Build**

As with most IT projects, a telecommuting initiative should go through a build vs. buy analysis to determine the best course of action. Key to this decision is the CIO’s methodology for using internal staff. Often, CIOs prefer to use their internal resources to deliver applications and technologies that create a competitive advantage. They may select to outsource infrastructure and communication services to providers who can offer best practices, economies of scale, and a track record of success. Managing the myriad of last-mile vendors, coordinating circuit installation, configuring and deploying equipment, maintaining CPE replacement inventories, deploying performance monitoring tools, managing security, fielding user support calls, and creating associated training can be daunting tasks. Partnering with a provider who has successfully implemented other telecommuter programs and has existing relationships with last-mile providers, equipment vendors, and field service resources can often reduce project risks and speed up deployment. Working with a provider can also help quantify and guarantee service levels and deployment costs. Often, providers can help CIOs better manage costs by reducing the upfront capital expenditure costs and integrating all elements into a user-based, variable cost model for more control.

A decision to engage a VPN service provider should be made with care. Interview multiple providers and their existing accounts. Make sure that the provider can provide an automated broadband VPN provisioning, monitoring, and management plan. Be sure the provider is more than a broadband aggregator, and operates an IP backbone and a 24 / 7 / 365 network operation center. The provider should also offer flexible options for growth, including site-to-site VPNs, Internet access, and security services. Be sure that the provider has strong SLAs with clear metrics and financial penalties. These SLAs should cover more than network availability, but should also address individual customer circuit performance, provisioning times, problem notification/resolution, and web-based reporting.

## Conclusion

---

Regardless of whether implementing a telecommuting initiative with internal resources or an outsourced partner, the core components of a successful project remain the same. Clear communication and training, proper expectation setting, reliable technology, and passionate project leaders are paramount to achieving the mission. With the right planning and consideration of the issues outlined above, you can ensure that your telecommuting program is a success.

©2011 MegaPath. All trademarks and service marks are property of their respective owners.