Telecommuting Sound Practice Guidelines

Prepared by the

SIFMA Critical Infrastructure Sub-Committee

March 2009

Table of Contents

Overview

The SIFMA Critical Infrastructure Sub-Committee in conjunction with the SIFMA Best Practices Sub-Committee compiled Telecommuting Sound Practice Guidelines for the financial services industry and to assist member firms in the planning and execution of alternate work arrangements.

Although working off premise has been a standard among technologists, and certain key support and management personnel, enhanced planning for a greater number of staff to facilitate significant incident management, part-time support, and to support the general changing industry landscape needs to be considered in the current contingency planning model.

The support for an expanded off premise workforce, either temporary or extended, will require more stringent safeguards and controls over the availability of secure services to handle trading, settlement processing, books and records, documentation and confidential information. Several member firms have provided their Telecommuting procedures. This information was compiled as a best of breed suggested Telecommuting Sound Practices guide for member firms to use in their planning process.

Legal Disclaimer

This document presents guidelines that can assist in the establishment of a comprehensive business continuity program. It is not intended to be an outline of a business continuity plan or as a single best approach, but rather it should be viewed as a summary of significant components that an organization may wish to consider when developing a full business continuity program. The plan itself is but one component of the program. Organizations may also consider executive support, policies, measurements, maintenance, and reviews of the plan that constitute the program.

SIFMA does not guarantee the accuracy of any portion of this document, and does not assume any liability for any inaccuracy or omission in this document. This document should not be construed as legal advice. Readers are advised to consult with counsel regarding the relevant requirements for business continuity plans, prior to adopting any such plan.

1. Telecommuting Agreement

As there is a continued need to prepare for incident response and the continued expansion of an off premise workforce, many controls and standards need to be addressed. One of these standards can be a telecommuting agreement designed to establish a set of controls for both the firm and the telecommuter worker.

Telecommuting Agreements establishes not only a standard for alternate work arrangements, it also sets a code of ethics for each employee to follow. These agreements need to follow each organizations policies and procedures and may differ in overall scope. As such it is recommended that these guidelines follow the firms appropriate approval process.

A. Disclaimer clauses

- Duration of Agreement
- What governs Telecommuting Arrangements
- Policies and procedures
- Code of conduct
- Benefits and Policies
- Work Ethics
    - Hours
    - Overtime
    - On-call

B. Firm Disclaimers

- Rights to terminate arrangement
- Right to establish and schedule for hours

C. Agreements

- Provide uninterrupted support
- Employee provides necessary and proper care of children and family
- Due diligence in establishing vacation scheduling and gaining pre-approval from your manager
- Notification of sick time

D. Remote Storage Devices

- Review your firm's policies and procedures for use of devices such as, but are not limited, to USB file storage devices, E-SATA disk drives DVD/CDROM writers and personal communication and entertainment devices.

- Obtain explicit management written approval, as well as, approval from Data Security/Info Risk for use of any storage device. Any approved storage device should contain firm approved encryption and will only be granted on an exception basis.

- Risk-based controls and procedures should be deployed to ensure that such devices are used only for explicitly approved purposes, and that the data held on the devices is appropriately protected.

E. Signature and date

F. Request for Telecommuting Arrangement (Form)

- Date of Request
- Requestors Name
- Requestors Dept./ Business Unit
- Requestors Manager's Name

G. Managers Submission Section

The above named individual is requesting the following type of Telecommuting Arrangement(s) as a change in the regular work schedule.

- ☐ Flex-time Arrangement
- ☐ Telecommuting Arrangement
- ☐ Part-time or Reduced Work Assignment Work Arrangement

[Please complete the following charts to represent the current standard work schedule for the position and the proposed standard work schedule.]

Current	Monday	Tuesday	Wed.	Thursday	Friday	Sat*	Sun*
Standard Hours							
Location							

Proposed	Monday	Tuesday	Wed.	Thursday	Friday	Sat*	Sun*
Standard Hours							
Location							
_____% reduction from a full time assignment (if applicable).							

H. Duration of Telecommuting Arrangement

Number of Months: _____ (Not to exceed _____months)

Start Date: _____ End Date: _____

*Note: Saturday and Sunday workdays are not available in all areas

2. Equipment Requirement

Firm's develop their own internal policies to define and determine how an employee gains access to its networks when required or permitted to remotely work from home or another location, as well as what they can access and when. For many firms, only computers supplied through a firm are permitted to access critical data for processing and reporting purposes.

For those firm's that elect to allow personal computers to access a firm's network for critical business activities, firm's may wish to consider stringent guidelines be established with regard to type of computer, operational and protection software that can exist.

These same rules may apply to preferred equipment that an organization may consider unique for a particular employee, and may be needed to facilitate alternate work support.

Below are sound equipment requirement practices that firm's may wish to consider:

A. Company Supplied and Verified

- Only Firm owned laptops with approved software may be allowed.
- Access to networks will follow firm established policies and procedures.
- Only use Firm provided computer to access the network from a wireless router and network modem.
- Only connect bank approved peripheral devices to the laptop (such as printers, scanners, fax, copier)

B. Non-company provided hardware

- Privately owned computers that will be approved for network access should be no older than 3 years to support company approved software.
- Any application software and virus/firewall protection should be installed by your firm and tested.
- Access to networks will follow firm established policies and procedures.
- Only connect bank approved peripheral devices to the laptop (such as printers, scanners, fax, and copier).
- Based on data sensitivity firm encryption of data would prevent unauthorized individuals from viewing information.

C. General Sound Practices

- If an employee is identified as designated for work recovery, they are required to have a tested working environment within a reasonable period of time.
- Telecommuting work sites are expected to be maintained and tested on a regular basis
- Follow the firm and divisional policies that require confidential and proprietary materials.
- Contingency provisions should be considered to have alternate staff in the event that a designated employee has to be evacuated from their alternate work location.

3. Guidelines for Off- Premise Workforce

Working remotely has been an opportunity in the technology field for many years and in recent times has been available for key personnel. When we look at the prospect of a large number of personnel to have the capacity to support a firm's ability to meet critical time sensitive business processing in the event of a long term disruption many issues come into play. In order to meet this need Business Continuity (BCP), Technology, Compliance, and Regulations, where applicable, may wish to consider developing standards and guidelines to the alternate work environment as well as identifying priorities for access.

Telecommuting Arrangements may involve working at any non-firm location such as remote from home, working-in-transit, etc. Employees need to be diligent and responsible to protect personal and sensitive information regarding customers, company and employees regardless of their work location.

Telecommuting Arrangement Sound Practices:

When employees are given the opportunity or are required to work from alternate locations, there are many considerations for both the employee and the firm that need to be addressed. These considerations include user responsibilities, required software, software licenses, anti-virus and firewall protection. Below is a series of best practices that can be applied to the employee and the business.

A. Employee Responsibilities

- Keep sensitive documents out of plain sight
- Avoid leaving sensitive information in areas where unauthorized persons may have access to it
- When not in use, and overnight, sensitive information should be stored in a locked file cabinet or desk

- Confidential data is not to be processed on employee personal equipment. In particular data relating to identifiable staff and customers should not be processed on employee personal equipment. Confidentiality of firm data, clients or employee data is of utmost importance and is not to be taken lightly.
- Be aware of surroundings when discussing sensitive information and of anyone shoulder surfing and trying to look at your screen or documents
- Do not leave your laptop out overnight for an extended period of time in unattended workplaces
- Connecting to your firms business network through a wireless LAN should only be done through the use of a computer and wireless card provided by your firm
- Connect only approved peripheral devices to your laptop (such as a printer, fax, scanner copier)
- Avoid printing information whenever possible.
- Any printed documents that you discard should be shredded
- Approved landline telephones should be traditional(non-cordless model)
- Employees should understand bandwidth implications for the business activities they are performing. Synchronizing files locally over remote access, accessing media reach (news and other informational) web pages or viewing videos could slow other more vital communications. For example, down loading a large e-mail may interrupt or distort an IP voice call or delay market data to a trading application. Employees should consider the use of bandwidth saving practices (i.e. use of compression techniques such as zip files, convert frequently accessed corporate web pages to text-based)
- Consider using instant messaging and two way pager services in place of voice communications
- Use care when opening and downloading attachments to ensure that they are virus free
- Employees are responsible to ensure their internet service provider has the proper resiliency needed to support your business contingency plans and work at home strategies. It is also recommended that critical staff have either a wireless air card or some other type of internet service satellite dish network (e.g. Hughesnet, Direct TV, Dish…). Critical users should attempt to remove any potential single points of failures that could prevent access. It is also recommended that critical users consider backup power for home use.
- Where possible limit the size of email attachments. If for work there should be a shared location where you can have documents reside for internal access.
- Log-off company network when not performing work that requires access
- Make sure that you abide by your firm's firewall guidelines when receiving and transmitting data
- Make sure you have emergency help numbers readily available,i.e. Help desk
- Avoid non-critical use of the internet, wire line or wireless networks
- If work permits, establish flex-time arrangements by function and time critical activities

- When using personally owned equipment to access Firm provided applications, the user takes responsibility for support of any non-Firm provided software and solving any issues related to access.

B. Firm Responsibilities

- IT staff may need to access IT infrastructure remotely. Businesses should consider procuring dedicated support tools to allow IT staff to monitor, troubleshoot, and configure IT infrastructure from remote connections. These remote capabilities should be provided with dedicated equipment to prevent these critical users from facing congestion. For example, a business could reserve ports on modem pools exclusively for IT staff as a backup method in case of congestion in VPN access.
- Businesses should consider developing policies that will delineate clear organizational ownership for managing privacy risk for corporate and individual data
- Businesses should consider developing guidelines for telecommuting which should include guidance associated with the businesses needs and risks, for all employees, including full-time, part-time and contractors
- Business should consider developing formal policies, operational procedures or training in order that all employees are educated about the risk of data loss, the risk of breaches of privacy or security surrounding personal information
- Business should consider clear, consistent background screening for all full-time, part-time and contract workers who telecommute and who have access to other individual personal information
- Business should consider developing credentialing guidelines, by employee job function, which addresses varying levels of risk associated with telecommuting. The ability to monitor the employee activities should also be considered.
- Businesses should consider developing guidelines for the protection, use and disposal of paper records in order that telecommuters understand the need for protection of paper records containing personal information
- Businesses should consider requiring wireless security measures such as Wired Equivalent Privacy (WEP) and WiFi Protected Access (WPA), as well providing direction to employees on how to secure their wireless networks at home
- Businesses should consider identifying physical security requirements for telecommuting employees, such as failed login lockouts on computers, privacy screens, house visits for audits of telecommuter physical working environments, security cables to lock down computers, etc.
- Businesses should consider hard drive and email encryption tools for telecommuters, as well as guidance on proper use of the tools, however, difficulty arises when employees are using their own personal computer
- Businesses should consider evaluating Internet bandwidth requirements at enterprise gateway routers for peak usage projections. Reviewing telecommuting traffic during winter

storms or other scenarios in which the office was closed may provide insight into increases in telecommuting demand that may be seen during peak usage.

- Businesses should consider investigating redundancy and diversity for their Internet connection. A dual Internet link provides redundancy and using separate Internet providers may increase diversity. When investigating a dual link, physical diversity should be examined as well.
- Businesses should consider assessing their ability to support potential increased teleconferencing demand by working with the service provider who manages the teleconferencing services. Businesses should consider structuring their contracts to accommodate additional audio/web conference ports to support the increased demand during periods of peak usage.
- Businesses should consider providing employees with multiple options for remote connectivity (e.g., Internet VPN, modem pool, iPass backup to modem pool, services that do not require VPN). Diversity of remote connectivity options can mitigate the effect of technical issues related to any one remote connectivity option. Telecommuters should be made aware of the remote connectivity options and should understand how network performance may be different with each technology.
- Businesses should consider encouraging critical employees to obtain multiple connectivity options such as DSL, Cable, Fiber optic, Satellite etc.
- Businesses should consider developing the ability to monitor, limit or turn off remote access capabilities. Under certain Regulatory and Firm Guidelines, Core or Blocked Leave may require certain "sensitive" employees to take 10 consecutive business days as leave away from the firm. During this leave period," sensitive" employees, should be both "off-site" and "off-line." As such, "sensitive" employees should not be able to conduct, or direct others to conduct, business. During the Core or Blocked Leave period, firms should consider monitoring, limiting or turning off remote access capabilities.
- Businesses should consider developing a remote access prioritization list. Firms may have more remote access users than the number of concurrent user license capabilities in place, as not all users are ever anticipated to utilize the remote access service concurrently. Firms should consider ensuring that critical staff will have remote access capability during a crisis and that bandwidth, in the crisis situation, is not utilized by non-critical staff. Therefore, firms should consider developing a prioritization process that will enable critical user's access during a crisis and disconnecting or blocking non- critical staff remote access capability.
- A personal desktop should be reviewed by the firm's security group who should remotely install all the necessary firm approved security for connectivity into the firm's network, such as access entitlements up to date virus software.
- Personal home computers for telecommuting should meet company standards for replacement, which generally fall within a 2 to 3 year period
- Businesses with critical telecommuting needs during a potential situation should consider working with network providers to obtain to obtain dedicated services for critical employees
- Make sure you have established Telecommuting arrangements in advance by incident and have established a published list for management and technology support. Establish procedure to add or subtract from the approved list.

- Remote PC's should use an operating system compatible with the Citrix or other Application Servers if the web is to be used for connecting to the Firm.
- Only active users in the Firm will be authorized for access. As a user, you are required to log in and test connectivity within 30 days after receiving an access token or service will be removed
- Consider managed internet access for critical personnel
- If either customer or bank sensitive information is kept at home on a regular basis line management should consider whether the employee's home should be fitted with a proprietary intruder alarm. Where this cannot be satisfied consideration should be given to refuse working from home.
- For those critical employees targeted for telecommuting should install a dedicated line for firm business.
- Telephone service should not be provided by internet providers, i.e. Optimum, Vonage, etc. as internet bandwidth issues could occur impacting telephone usage. Landlines are the preferred telecommunications option
- Mobile phones should have additional battery packs sufficient to carry 72 hours of normal use.
- For seamless communications you may be required to have handsets attached to lines programmed to display your firm's caller ID info for sales and marketing calls.
- In the event of large data transmissions, where possible, receive or transmit in non critical or off hours.
- Be prepared to stagger your activity on-line to reduce peak traffic flow and priority processing.
- Ensure that Telecommuting contingencies are regularly tested during test cycles.
- Employers could consider assisting employees in improving their remote access practices by implementing compression technologies, minimizing the media content of internal web pages and using network options (such as Quality of Service to either demote or promote communications based on the connection importance and the potential sensitivity to congestion) to enable more efficient content delivery to telecommuters. Use of compression tools, such as Zip Files, for large attachments, such as PowerPoint presentations, can significantly reduce file size and allow for faster and more efficient delivery. Another option is to use documentation and collaboration tools such as Microsoft SharePoint or even shared drives to centrally host documents. Links to these documents can then be circulated via email instead of the documents themselves.

C. Software

- Any software installed on your personal computer should be consistent with the firm's standards.
- Make sure software patches are updated on both your personal and company computers

D. Licenses

- Most personal software licenses either expire after 1 year or are remarketed with updates. For those that expire you should always renew this license when prompted. Before you upgrade any software packages, ensure that they meet the operating standards of your organization.
- If software installation on your personal computer is a requirement of your firm than you should have them provide the software and necessary updates and patches under their standard global license.
- Ensure that computers provided by your organization can be accessed for updates or software changes under the firm's license agreements
- Operating software should always be consistent with the firm standard

E. Virus and Firewall

- Regular updates to antivirus software should be installed on your personal computer
- For proper firewall protection a firm provided router with access security and a secure ID access token should be provided to the employee
- Be mindful of announcements and automatic updates from computer and application vendors.
- Ensure that virus software is always up to date
- Ensure that employees understand the risks of opening and downloading attachments to ensure that they are virus free
- Make sure firm's firewall guidelines are available to the employee for receiving and transmitting data
- For telecommuting arrangements, make sure you use strong passwords to avoid intrusion
- Make sure, if using personal computers that you establish physical access to block intruders
- Regular updates to your personal firewall should be installed on your personal computer. Personal firewalls can protect the integrity of a connected computer by filtering network traffic, and alerts you if an "intruder" is trying to access your computer

4. Guidelines and Sound Practices for fees and costs associated with off-premise expenses

When selected as a telecommuting personnel, there are many issues surrounding to what extent the firm or you are required to cover expenses associated with the establishment of an alternate work location. A lot depends on what each firm will require versus what you have in place.

A. Examples of Covered Expenses

- Dedicated network services
- Dedicated telephone lines
- Firewall Routers
- Required telephone service i.e., traditional (Verizon, ATT, etc) versus an internet provider, i.e. (Optimum, Vonage, etc)
- Additional battery packs for Mobile phones for extended emergency usage.
- Home based employees may be eligible for reimbursement of one time and reoccurring related expenses. Handsets attached to these lines should be programmed to display your firm's caller id info for sales and marketing calls.
- If determined critical the installation of multiple connectivity options; DSL, Cable, wireless broadband, satellite and land-line telephones should be provided by or paid by the firm
- Any required equipment that is defined by the Telecommuting agreement could be subject to reimbursement, such as a Shredder, fax, copier or printer if your personal equipment does not qualify for network connectivity

B. Examples of Expenses not covered

- Your personal Computer
- Your current internet service provider
- Your current telephone service provider
- Existing support equipment, printer, fax, copier
- Non approved software

5. Off Premise Trading – Points To Consider

Trade execution falls under extreme scrutiny to ensure clients receive best and timely execution price first and foremost to any firm activity. For this reason the industry as a whole has been considering of off-premise trading.
There are many issues that need to be addressed in this area, but for planning purposes below are some of the best practice points to consider.

A. Equipment Requirements

- IP based Physical turret
- PC based "soft" turret
- Laptop
- Mirrored image of employees applications
- Monitors

B. Software requirements by trader

- Need to ascertain if trader working in Risk Mitigation vs. Business Continuity mode to ensure what applications are required for access

C. Market data requirements by trader

- Need to ascertain if trader working in Risk Mitigation vs. Business Continuity mode to ensure what applications are required for access

D. Security

- Secure ID authentication into authorized server
- Enhanced security required allowing access into remote desktop to remotely control desktop pc. This access should consider the use of the firms user ID and password as authentication
- Enhanced information security to ensure "Users or external customers are who we think they are"

E. Broadband

- Assess broadband bandwidth to ensure required response time

F. Supervision & Controls

- Exception reporting
- Recorded line consideration
- Would trade reporting on ACT and TRACE timeframes be impacted
- Will books and records of firm be updated automatically with trades processed from home

G. Record Retention

- Ability to retain documents relating to business when trading from remote location

H. Regulatory and Compliance

- Possible registration of "Office" may be required
- Remote access should be used for business purposes only! Trading activity from remote locations is not permitted, unless Executive Management and Compliance have given prior approval and the Firm is operating in contingency mode. Any breach of this Policy will be treated as a very serious disciplinary issue and may cause termination of employment with the Firm.

I. Communications

- How will clients, brokers know how to reach various traders via phone

Note: the items above are not intended to address all Telecommuting Sound Practices just those specific to Trading from Home

6. Testing as Part of Business Contingency Planning

It is recommended to include Telecommuting Arrangements testing as part of your organizations recovery and testing cycle. The inclusion of this as part of the testing cycle will enhance recoverability from large scale incidents and should demonstrate the ability to support large scale off-premise network access and availability of applications during staggered hours. Proper preparation for these types of tests requires expected result targets within well scripted test documents, as well as coordination between the business units, technology, compliance and the BCP Staff.

7. Update Business Resumption/Disaster Recovery Plans and Procedures to reflect Telecommuting scenarios

Telecommuting Arrangements testing should have an expected result test script and the results of this segment of testing should be well documented. A post mortem review of the results will aid in the improvement of Business Resumption/Disaster Recovery plans and provide for solid in-house sound practice.

8. Priority Services

Dedicated or premium service should be considered by financial institutions to support critical services. Firms should consider arrangements, for critical employees supporting critical services, with telecommunication service providers, which can be activated during a pandemic or other disaster scenario.

These enhanced arrangements should be clearly defined by type of incident and firms should consider discussions with various providers to ensure that they can support premium service for deployment to identified employees to support critical processing.
Services to consider are:

- Private lines- a service to provide a dedicated circuit between a telecommuter's location and the firm's network. This provides dedicated connections with high priority service.

- Managed internet access- provides dedicated internet connections to allow telecommuters to bypass local congestion points which can potentially deny access. In a serious incident throughput can be affected by other congestion points and can still affect critical personnel access.

- MPLS and VPN's- addresses multiple service levels across providers which can be available through various remote access connections; i.e., dial-up, cable modems, DSL. The service could also include performance and availability guarantees through a managed arrangement.
  Even though this method provides for a multiple access alternative, MPLS VPN needs to travel through points of congestion.

9. Next Generation Services

In our current environment, national security/ emergency preparedness has given rise to enhanced voice telephony measures with the implementation of GETS and WPS. Although individually we need to plan for redundant and robust services, national security next generation of services should consider establishing best practices in the area of video conferencing, e-mail and internet access. This type of effort will not only aid in the control of cyber security and business and economic protection but will support priority and critical processing for several million alternate work personnel if a major incident occurs.