

RETURNING TO THE OFFICE: IT AND STAFF GUIDELINES

The pandemic continues, yet firms and employees are also planning how to safely get back to “business as usual.” Returning to an office environment requires careful planning, with the top priorities being employee health and safety, and compliance with [Centers for Disease Control and Prevention \(CDC\)](#) and your local official guidelines.

KEY CONSIDERATIONS:

Firms must consider multiple factors before initiating a return to the office:

- What are the firm’s responsibilities for employee health and safety?
- How many staff will be returning to the office?
- Who will be required to work in the office?
- Who can or should continue working remotely?
- What remote access procedures are in place?
- Can data integrity, confidentiality and security be preserved across all working environments?
- Are employee guidelines consistent, up-to-date and readily available?

In determining the next steps for returning to the office, your firm should first establish how many staff will return and who will continue working remotely, with clear criteria for making these decisions. Whether in the office or remote, all firms should have consistent protocols in place across the business. For employees working remotely, the firm should outline remote access procedures, particularly for the protection of confidential data and systems.

FOLLOW OFFICIAL GUIDANCE

Firms must comply with official restrictions and should update staff regularly on guidance from the federal, state and local governments.

Industry bodies such as the [Occupational Safety and Health Administration \(OSHA\)](#) and the CDC are an additional source of important information. According to CDC guidelines, businesses with employees returning to the office should implement a number of safeguards to combat the spread of COVID-19.

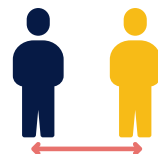
These include:



Use of healthy hygiene practices



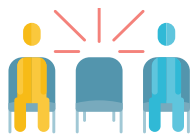
Intensified cleaning, disinfection, and ventilation



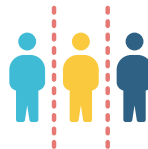
Social distancing



Telework and cancellation of non-essential travel



Seating distance of at least 6 feet and staggered gathering (start/closing) times



Restricted use of any shared items or spaces



Training all staff in all safety actions

Management should also understand the firm’s responsibility and liability in asking any employee to return to the office, either through their HR and/or legal team or partners.

VENDOR PROTOCOLS

As employees return to the office, management should implement protocols for vendors and guests visiting the office in-person. Here are some practical suggestions for maintaining social distance guidelines during in-person visits:

- **Mail deliveries** (UPS, Fedex, Amazon, etc.) – place a drop station in front of the main office door for mail/package drop-offs
- **Guests** – if you have clients or other guests visiting, designate/allocate one area of the office for meetings in order to eliminate extended contact in common areas, e.g. a designated conference room
- **Kitchen safety** – replace reusable glassware and silverware with single-use plastic and paper plates and cups, especially with guests



COMMUNICATION

With some employees continuing to work remotely, firms must implement clear rules for both internal and external communications. Questions to consider include:

- What methods of electronic communication will be appropriate? Email, Phone, Instant Message, Text? Are they secure?
- For registered entities, are all means of communication being archived in compliance with [SEC guidelines](#) in Smarsh, Global Relay, Slack, Microsoft Teams or other means of communication?
- Have you updated your business docs (e.g. compliance manuals, DDQs, BCP, etc.) to reflect these changes?

TECHNOLOGY PROTOCOLS

In order to ensure all employees are equipped with secure, robust technology, firms should first evaluate how employees have fared while working remotely. If your IT operations and network connectivity were limited over the past few months, it is worthwhile considering working with a [technology partner](#).

IT Infrastructure providers, particularly those working in the public cloud, can help your firm better determine the right tools and protocols to implement as employees continue to work remotely. Additionally, your technology partner can help your firm transition back to the office, securely and efficiently.

Your technology partner can help your firm address a number of key questions:

- Have you revisited your data structure and permissions to network resources/files?
- Were there ad hoc changes made to access files or an overall network, such as establishing a VPN from a home computer, for example?
- Have controls or procedures been set for handling data while remote? Are protocols and backups in place to ensure data and files are saved and accessible within the company's domain, not just on an employee's local PC? How will this be monitored?

MOVING FORWARD

As you take your first steps in returning to “normal”, you will likely focus on strengthening your business in the process, and evaluating where you might need support. At Siepe, we help firms implement secure, resilient and nimble IT infrastructure and software solutions that scale with your business. Our staff of experienced and capable IT professionals delivers efficient and effective IT solutions designed specifically to meet the requirements of financial service firms.

[Contact us](#) today and learn how we can help address your firm's technology needs, for the short- and long-term.

