Stapel Managed Service On-boarding Checklist

The Stapel on-boarding process is extremely important. Technology is Information and it is key to building Your Technological Foundation. Based on the availability of information, the Stapel on-boarding process should be expected to take place within a 4-6 week window depending on the services we've partnered to provide. Please refer to the outline below for an overview of our on-boarding process.

1. Week 1-2: Setup
   a. Back Office Setup
      i. Stapel will setup the agreement in our system and generate the initial invoice(s).
      ii. We will work with you to schedule a date and time for the initial on-boarding call.
      iii. During the initial on-boarding meeting, we will discuss payment arrangements with you for the agreement.
      iv. We will prepare the on-boarding timeline for our initial on-boarding call.
   b. We send you a link to install our remote monitoring and management agent
      i. The remote monitoring and management agent is installed on a server or designated machine within the customer environment. From this point, the agent is deployed to all other machines in the environment.
      ii. For machines that may be remote, the download link can be shared with those users for them to install individually.
      iii. Detailed information about each machine is automatically sent through agent software, and recorded in secure Stapel databases. With these agents in place, we will be able to gather valuable information about your environment.
      iv. Once the agents are installed on the machines, we can immediately begin troubleshooting any basic issues that your users may be experiencing through our Help Desk - even before the on-boarding process is entirely complete.
      v. All additional services will be configured within 48 hours of successful deployment of agents to each machine within the customer environment.
   c. You review and complete the [Getting Started Checklist (Below)](#)
      i. We encourage you to complete the Getting Started Checklist to the best of your ability. This document will assist you in gathering necessary files, paperwork, and information regarding your current network. Completing the guide is beneficial to all parties and will save a great deal of time during the Stapel systems auditing process.
      ii. If there is anything on the checklist you need assistance in gathering, please reach out to your account manager and we will get the necessary resources involved to assist.
2. Week 2 – 3 Kickoff
   a. Schedule Stapel onsite visit
      i. The length of the onsite visit greatly depends on the size of your organization, however, is typically completed in one business day or less by our technicians.
   b. Follow-Up Meeting with the customer

      i. Your account manager and an assigned technician will meet with the you to discuss the **Getting Started Checklist** and work with you to fill any gaps.

      ii. Our technician(s) will tour your office so that we can gain an understanding of the floor plan and note specific locations of critical network hardware.

      iii. Throughout the onsite visit, our technician(s) will gain an understanding of your common issues or concerns regarding your IT environment.

  c. Additional onsite work and processes

      i. We will perform detailed documentation of all hardware and the physical location of each device.

      ii. Any configuration changes that were identified as beneficial will be performed during the initial onsite visit.

3. **Week 3 +: Customer Services Implementation**

  a. We begin to roll out your services in order of priority to you. This is determined during those first couple of weeks of reviewing your environment and discussions with your team regarding your priorities.

  b. The remainder of the on-boarding process can be done remotely and behind the scenes.

      i. Finalizing documentation of your environment in our systems

      ii. Creating administrative accounts for Stapel to use in your environment

      iii. Installing various services such as Antivirus and Remote Backup

      iv. Implementing best practice configurations for existing services that will remain in your environment.

We will agree on a "Go Live" date based on progress and work with you to communicate to your staff everything they need to know to officially start taking advantage of Stapel Support Services.

Thank you for your business and we look forward to becoming *Your Technological Foundation!*

Stapel Service Getting Started Checklist

☐ Floor Plan of your business suite:

Please provide a basic floor plan of your business suite, identifying each workstation. We ask you to label each workstation with the current user's name. During our onsite audit, we will edit the floor plan to include additional information.

☐ Access to your office and server room:

In the event we need to be onsite during non-business hours, we will need access to your office and infrastructure areas. Please be prepared to provide some method of entry, such as keys, key cards, combinations, or security codes that may be needed to access these areas. You will be notified prior to our entry into a secured area.

☐ List of employees:

To streamline communication between our technicians and your users, we request a detailed user list. Please include the following information for each employee that will be supported.

- First and Last Name
- Email Address
- Direct Line or Extension
- Cell Phone Number
- Title
- Location/Workplace Address (Particularly for remote employees)

☐ Billing and account information for technology services:

We request a list of service providers, complete with contact information and service account numbers, to increase the efficiency of our troubleshooting process and assist in managing the vendor relationship. Please have a copy of your most recent statements from the following service providers:

- Internet Service
- Domain Name Registrar
- Hosting Services
- Email
- Phone Provider
- Any Software Vendors that are central to your environment
- Any network based leasing agreements, for example copiers

☐ Documentation from previous IT vendor(s):

Your previous IT vendor(s) should have returned your network documentation. Having this information will give us a head start on our audit. Stapel will verify the accuracy of all information provided.

☐ Domain Administrator Account credentials:

We will need access to your network to create an administrator account. This will allow us to install our software and assist you with your IT needs.

☐ Usernames and passwords of network devices:

Please provide us with usernames and passwords to your various hardware devices, for the following types of devices:

- Network Storage Devices
- Printers
- Wireless Access Points
- Firewall
- Internet Modem or Router
- Network Switches
- Backup Devices

☐ Basic workstation configuration:

To successfully manage your network, we need to collect some general information about the computers and preferred settings within your work environment. This will help us in the future when configuring new computers that you may purchase. We understand that various users or departments may have specific configuration needs, so the more detailed information you provide will allow us to better understand your environment. Please provide the following information:

- Do your users share a printer?
- What version of Microsoft Office are you currently using?
- Do your users regularly use any programs or applications other than those included in the Microsoft Office Suite?
- Endpoint security solution including Antivirus or other security applications in the environment.
- Please provide the names, license keys, CDs/DVDs, and any additional information you may have pertaining to each application used within your environment, including your Microsoft Office Suite.

☐ Mobile device information:

To best serve the needs of users within your environment, we need to know if your employees use phones, tablets, or other portable electronic devices to work remotely or send and receive company email.

- If your employees are currently using mobile technology to access company email, are they using personal or company issued devices?
  - What types of devices are currently being used by your employees for this purpose?
- If your company does not currently use mobile technology, please let us know if this is something you would like to implement in the future.

☐ Wireless information:

Do you have a wireless network in your office? If so, please provide us with the network name and password. This will help our technicians access the internet with our laptops while onsite and help build our documentation on your network for future support.

☐ Remote Access:

Please let us know if your network is configured to allow users to work from home, or another offsite location.
- If you can access your network while away from the office, please let us know the steps you take to do so.
  - Does your company use Microsoft Terminal Services, VPN Client Software, or something else?
- If you company does not currently have the capability in place to work remotely, please let us know if this is something you would like to implement in the future.

☐ Backup/Disaster Recovery Environment:

We will need details regarding your current backup infrastructure, including the following details:

- Software or solution used
  - For local backup solution, we will need access to the local infrastructure.
  - For online or remote solutions, we will need credentials to examine the configuration/setup so that it can be documented
- Backup Storage Location
- Frequency

☐ List of common/recurring complaints or issues related to your technology:

Most companies come to us with a "laundry list" of complaints related to their network, mobile devices, and computers. We encourage you to compile a list of these concerns, identifying the user(s) experiencing the problem, so we can efficiently and effectively address the needs of your employees. Using this list and the results of our initial audit, our technology experts will be able to resolve your noticeable problems with the highest level of priority.