

What to Know When Changing IT Service Providers

A Checklist for IT Managers, Directors, Executives, or C-Level Employees

SynchroNet is a specialized provider of professional and managed IT services for mid-sized enterprises and small businesses preparing for growth. For over 20 years, we've been helping companies use technology to optimize the productivity and profitability of their businesses while alleviating the risk of service disruption. If you are thinking about transitioning to a new IT service provider, please feel free to call for our advice at 713.574.8200 or visit our website at www.synchonet.com for more information on our company.

- 1. Take inventory.** Take the time to document all hardware and software that your company owns. Some IT companies offer Network Health Assessment services – which provide you with a document containing a list of all your network devices, licenses, operating systems, and any programs that are unique to your organization - along with the associated “wellness” of each component.
- 2. Know who has rights.** Know all of the passwords to every secured device. Know who has access to data and the passwords that protect it. If these passwords are documented – find out where. Your company's financial, customer, and legal information is extremely private, and should be treated with great care. After you successfully make the transition to a new IT support company, change your passwords.
- 3. Documentation.** All documentation, configuration, and installation disks for hardware and software should be collected, cataloged, and stored in one area. In this contained area, include all of the product license keys and purchase information for all software that is running on your network. (This will benefit future troubleshooting, as well as peace of mind – in case your IT systems are ever audited.)
- 4. Compliance.** If your organization has strict compliance regulations, make sure that the new IT service provider can support these enforcements for your company.
- 5. Internal Security.** Most business network attacks come from internal users, not outside parties. In order to ensure your company's protection, you should have a written record of security products and procedures – including a document of policies for employees.
- 6. Know EVERYTHING about your backups.** The backbone and most critical aspect of your business is your data. It is essential to know everything about your backup system, and to ensure that all of your data has been secured.
- 7. Maintenance.** Is your current IT provider conducting daily/weekly/monthly updates to any portion of your network? If so, you will need to know the details of these procedures, and make sure that your new IT service company can provide you with the same level of assistance.
- 8. Know your contacts.** Now is the time to make sure that you have a comprehensive contact list that includes the names and information of all of your service providers: managed services, telephone, data, web hosting, etc. You may also find it helpful to create a binder which includes all of the service agreements associated with each of these providers. Make an effort to contact each provider and make notes of the level of response you receive from each company.