10 Important Documents Your IT Managed Services Provider (MSP) Should Maintain (And Be Easily Available!)

It never ceases to amaze us how many clients we take on whose previous IT Managed Services Provider (MSP) failed to maintain even a basic level of documentation on their networks. Without detailed documentation, IT engineers will be relying on their memory or the memory of their colleagues or even the memory of the client(!) for crucial information which will inevitably lead to mistakes and delays when dealing with service requests. They will also be unable to take a holistic view of all systems when reviewing IT strategy and security.

Usually, with the in-depth Labyrinth Technology initial on-boarding survey, we are able to gather most of the information we need to build our enterprise level documentation pack. But often we find that passwords to routers, SANs, access points etc are nowhere to be found, leaving us with no option but to complete a factory reset on these devices and start from scratch. This is usually a good indication that no maintenance was being carried out. (e.g. routine firmware upgrades/security patches), which on the one hand means we can ensure everything gets put right, and performance/security issues are

dealt with, but on the other it's a delay to completion of the project due to a lack of basic care on the part of the previous MSP.

Regardless of how large or small your organisation, and irrespective of the business sector you operate in, these documents are vital - particularly if your IT Managed Services Provider is supporting and maintaining many different networks. **And remember**, it is just as important to implement some sort of procedure or system for updating these documents/systems and handling the necessary change & version control (we use SharePoint which automates this).

So here is a list (in no order of importance) of some of the most important network documents that either your outsourced IT department should be **creating** and **maintaining,** and that you should be **easily able to access** for whatever reason. This is all standard information that we gather and maintain for our clients and can produce at any time.

1. **IT Systems Documentation –** Whether created as individual documents or one super document, it is important that there is a record of key information on core services and infrastructure, including but not limited to; network, servers, backup, cloud services and business applications. Any future employee of your incumbent or future MSP should be able to pick up this documentation and get a good understanding of how everything is set up, as well as (very importantly) contact details for any 3rd party suppliers.
2. **Change Control Register –** Without keeping track of all significant changes to your overall IT systems, it will be very difficult for your MSP to determine what has recently changed that could be contributing to a problem or issue, or be necessary information to all for the smooth completion of an upgrade or installation. Typically changes will be tracked through a helpdesk system (and the version control on your IT systems documentation).
3. **Software Asset Register** – A detailed document detailing all software assets and where they are being used should be maintained. Without it, there will be no record of what software you have, who is using the licenses (and how many there are) and how to activate it when you come to reuse it for another user or device.
4. **IT Hardware Asset Register –** It is of obvious importance to track all IT hardware assets, so there is an up to date record of what there is and where it is. Without this, it will be difficult to review the suitability of expensive hardware to be purchased, you may end up overspending on equipment that you do not need because a suitable alternative is already on site, and there is no way to track that you have everything you believe you have (preventing theft, unreported loss or damage). We assign asset tags to **all** of the client devices that we manage and use an asset tracking system which automatically pulls detailed information on hardware and software installed for each computer.

5. **Secure Configuration Documents –** There should be a documented standard for creating user accounts, building servers and building computers which defines applications to be installed, services to be disabled, ports to be blocked etc. As the client, you should pre-agree this with your MSP and insist it is reviewed periodically in line with the latest security guidelines.
6. **IT Risk Register –** An IT Risk Register detailing all known risks, current controls and suggested controls should be created and reviewed regularly. The risks themselves will vary depending on your particular business sector, but could include risk to data, risk of financial loss and so on. Risks and suggested controls should be reported to you, ideally to your senior management team, on a regular basis.
7. **Logical Network Diagram –** This should show the IP addresses associated with different segments of your network. This is particularly important if you have different VLANs in use (Virtual Local Area Network) or a DMZ (a network area that sits between an internal network and an external network). Without this, it may be difficult for new MSP's or MSP employees to determine which IP schemes are in use and where.
8. **Physical Network Diagram –** This should illustrate the physical layout of your network such as servers, routers, firewalls, printers, computers and phones. **All** key devices should be listed. It may not need to list every single computer, but the diagram should give a good idea of how they are connected to your network.
9. **Static IP Address Allocation –** Your MSP should maintain documentation detailing all static IP addresses assigned to avoid creating an IP address conflict.
10. **Key Credentials Database –** Your MSP should maintain a **secure** database of credentials for key system accounts/devices such as routers, firewalls, servers.