The Best Practices for a Secure Network Infrastructure
When you run a business, the odds are that you are dealing with network technology in some manner. Whether your computer network is vast, or just a handful of devices, it is vital to secure the system to protect your business data.

The idea of creating a secure network infrastructure may be daunting. When broken down into steps, it is more straightforward than it might sound. Simply put, a secure network infrastructure is one that has systems in place to avoid threats. By identifying the things that could pose a security risk, and by addressing them proactively, you will ensure that your network infrastructure is well protected.

**Run a Risk Assessment**

Without knowing what potential problems exist for your network infrastructure, it is nearly impossible to take the appropriate steps to secure the system. One of your first steps in securing your network should be a risk assessment. This will determine potential problems in advance.

Consider all types of risk, from malicious human threats to physical problems with your space.
According to information security company ISACA, here are some of the most likely network security challenges businesses will encounter in the next 12 months:

- 13% Incidents from Employee-Owned Devices
- 17% Data Leakage
- 16% Employee Mistakes
- 19% All of the Above

Determine what steps, if any, have already been taken to mitigate these risks. Then, work to address any remaining risk.

**Train Your Users**

The weakest part of network infrastructure is often the people who are using it. All users need to be trained on best practices and updated on a regular basis. While people may not intentionally mean to cause problems, those who are not immersed in the information technology world may not understand how to deal with threats appropriately.

Your users should be trained on strong password use and you can enforce this through system rules. They should be aware of the impact of malicious links and malicious software, and know how to keep these things off your network. Train them, too, on what to do if they think there may be a security issue. This typically involves contacting the IT department or other appropriate experts, immediately, with full details of the incident.
Establish Authorization and Roles

Have different authorization settings for different groups. The IT department, for instance, should wield more power and have access to more files and systems than an employee who has nothing to do with network administration. Users should only have the permissions that they require. It is wise to protect your network infrastructure by regularly reviewing users and groups. Ensure that authorizations and permissions are still appropriate and remove unused accounts.

Keep Up To Date

When software and infrastructure are not updated, your network infrastructure can fail. It’s important to install updates and patches as required. They often address security bugs. If you don’t resolve these weaknesses in your system, they can allow unwanted access to your system.

Keeping infrastructure up-to-date is also important because outdated equipment poses its own problems. You don’t want vital hardware collapsing at the end of its life. Take steps to avoid this, particularly if you rely on that system for part of your network infrastructure.

Taking the time to update software and hardware regularly is a relatively simple way to reduce the risk of a catastrophic problem in the future.
Implement Firewalls and Virus Scanning Techniques

Protect your network infrastructure with a firewall, whether you choose a software or hardware setup to do so. Configure it appropriately for your system and test it. Once installed, it should always be in use.

Find appropriate virus scanning techniques for your system as well. Conduct regular checks for viruses and malicious software. This is especially important if many users have access to your system, as even the best user training may not protect you from errant downloads and other activities that can introduce human threats.

Create Strong Backups

If part of your system goes down, you lose data, or experience a disaster, it is vital to have critical data backed up somewhere off-site. This will allow you to restore access as quickly as you can. By having a robust backup system in place, you can achieve continuity and maintain the integrity of your network infrastructure in the event of a problem.
Check Your System with Audits

Having all of these policies and procedures in place is great. It is important to check in regularly, however, to make sure that your system is in good shape. See that it has all that it needs to be protected. Every time you add new software or hardware, or make other major changes to your network infrastructure, address how you will include these changes in your security setup. New staff and users should be trained as they come into contact with the network, to keep everyone at an acceptable level of understanding and competence.

Make security audits a routine, scheduled part of your IT management and administration. You will stand a better chance at finding potential problems before they can impact your system. Contact the network security specialists at IT Direct, and we'll help you identify and resolve any security risks for a more reliable, better performing network.