Data Security Best Practices

1. **Implement and maintain good PW management policies**

   Passwords should be at least 10 characters with a mix of letters, numbers special characters, and capitalization. They should be forced to change every 90 days.

2. **Implement and maintain comprehensive endpoint security on machines**

   You will need a good combination of tools including anti-virus, anti-malware, and ransomware mitigation.

3. **Maintain company-controlled system patching**

   Systems patching is critical and should not be left to the end users. Make sure the organization controls patching and related policies.

4. **Limit data access/permissions to "as needed" (or Least User Access, "LUA")**

   Make sure users have the minimum access and permissions they need to do their job. Don't unnecessarily expose sensitive data.

5. **Encrypt laptops**

   Laptops with hard drive will always contain company information. These devices can be easily stolen or misplaced. Encrypting laptops keeps your data safe and makes it harder to hack.

6. **Encrypt sensitive emails**

   Think of sending emails over the Internet like sending postcards by regular mail. If you don't want anyone to read it, encrypt it.

7. **Implement network based hardware security appliance (aka firewall)**

   Don't rely on an ISP's router to protect you. That's nothing more than a 'Do Not Enter' sign for a hacker. An integrated appliance that is constantly monitored and updated while inspecting ALL inbound and outbound traffic is a must. This device should also provide an additional layer of gateway anti-virus and anti-spam.

8. Educate your employees

One of the most important things you can do is continuously educate your end users on security policies and awareness. No matter how attentive you are to security, one click on a bad link can wreak havoc in your environment.

9. Backup Backup Backup!

Having a well-run backup process with adequate retention is critical in the event you have to restore damaged or stolen files. You must be sure to have a combination of on- and off-site repositories and enough retention to go back for several months if necessary.

10. Limit WIFI access

Make sure you keep your wireless access private with a secure password. The traffic should be encrypted and any guest access should be via a separate network with no access to critical systems and data points.

11. Implement a removable media policy

Create a policy and educate users on the use of removable media. The policy must work for the organization but can address such things as authorizations required, transfer of data and encryption.

12. Implement file retention policies

Create a policy and educate users on file retention. Keeping sensitive information around for longer than is needed creates unnecessary risk while eating up precious storage and backup space.

13. Implement asset disposal policies

Create a policy to govern the disposal of assets that may have sensitive data stored on them, such as old PC's and printing/scanning equipment. Assets should be disposed of with a service that will securely remove all data on such devices.

14. Implement HR policies for exiting employees

Create a policy to govern what happens to employee's data, accounts, and devices upon exit. Maintain an inventory of data storage devices for return, have a security lockdown process, and delete or move sensitive data, for example.

15. Use SSL on your web site

An SSL (Secure Socket Layer) certificate enables your site to encrypt traffic between your website and your visitors' browsers. Even if you don't transfer sensitive or proprietary information, it is a good practice since even user ID's and passwords could otherwise be seen. And now, not having an SSL can negatively impact your search engine rankings.

Get Enforce Managed Security FREE for a Whole Year!

For a limited time only, you can get our Enforce Managed Security program FREE for a whole year – with no set-up fees – when you sign up for our monthly Enable IT Service & Support program. These services combined will free up your business from dealing with everyday computer and network issues, and protect it from ransomware and other cybercrime.

See just how affordable it can be to have great IT service and strong, reliable network security!

Call 678-389-6200
mPoweredit.com