INTELLIGENT TECHNICAL SOLUTIONS

CYBER HYGIENE TIPS TO KEEP YOUR BUSINESS IN TIP-TOP SHAPE

Stay on top of your business management and technology tools

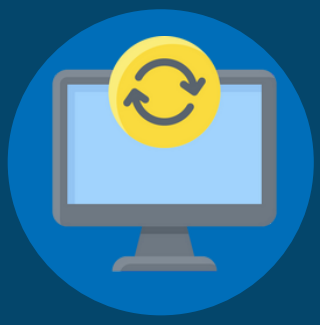
Identify, document, and analyze the hardware, software, and applications you are utilizing.

Completely wipe any hardware that you are not currently using

If you will not be using the equipment in the future, consider disposing of it.

Do a regular cleanup

Remove data, files, and information that is no longer needed to free up storage. In the same way, delete or uninstall any software or applications you are not regularly using.



Update your software

Update and install necessary patches for all software or applications that are in use-across all devices. Doing so ensures that your system is running the latest version and repairs security holes and bugs that have been discovered in the previous one.

Centralize existing applications

If you are using multiple applications to accomplish a similar function, consider streamlining and reducing duplicates.

Change passwords or passphrases at regular intervals

This might be the most common way to help secure your data. By regularly changing your password, you reduce the risk of someone else gaining access to your accounts. In addition to that, you should also refrain from using or reusing the same password across devices or services. Keep them fresh and unique.

Monitor internal security

Review the antivirus and malware software that is installed to ensure it is up-to-date and functioning properly. If, in any case, there's no antivirus and malware software at hand, review available options, and install immediately.

Incorporate multi-factor authentication (MFA)

And ensure your team members are using it. MFA enhances your organization's security by requiring everyone to identify themselves beyond username and password when accessing a company site or account.

Employ device encryption

This helps protect sensitive corporate data, both at rest and in transit.

Back up your data

Experts suggest following the 3-2-1 rule, wherein you store three copies of your data on two different kinds of media, with one copy stored off-site. It would be best to do this to an offline hard drive or to a secure cloud environment, whichever works for you.

Control access and authentication

Regularly review who admin privileges have been granted to and remove contacts that no longer need these privileges. Identify team members that have left the company in the past year and ensure their credentials and access have been shut down.

Develop an IT disaster recovery plan

This might be the most common way to help secure your data. By regularly changing your password, you reduce the risk of someone else gaining access to your accounts. In addition to that, you should also refrain from using or reusing the same password across devices or services. Keep them fresh and unique.

Host cybersecurity awareness training

Everyone's participation when it comes to the organization's cybersecurity efforts is critical to guarantee success. One way to do it is by holding quarterly cybersecurity training or sending out constant reminders.

Establish a cyber hygiene policy

Finally, draft a policy that details how to handle the above task and make sure to assign a specific person who will handle them.

INTELLIGENT
TECHNICAL SOLUTIONS