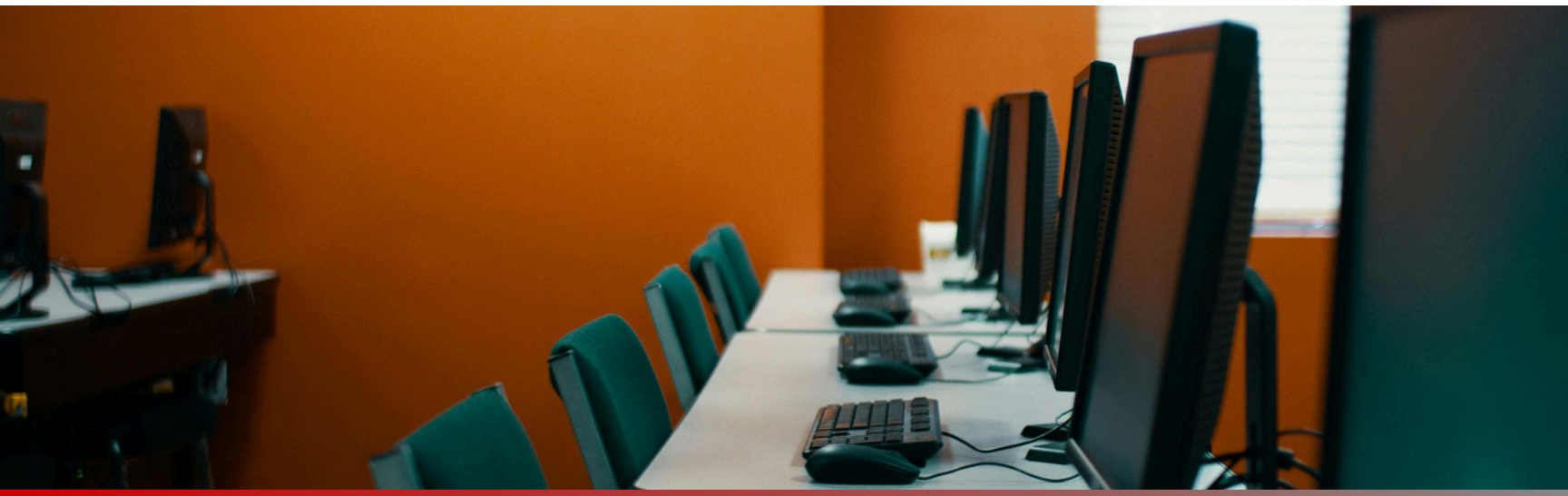
October 2026



TECH TALK

"Insider Tips to Make Your Business Run Faster, Easier, and More Profitable"

INSIDE THIS ISSUE:

Why Your Employees Shouldn't Have Administrator Access	Page 1	Why Guest Wi-Fi Should Be Separate from Your Business Network	Page 2
Gadget of the Month	Page 1	Small Business IT Budget	Page 2
Personal Devices for Work?	Page 2	How Long Business Computers Last	Page 2
When You Cancel a Cloud Service	Page 2	Technology Trivia	Page 2

We love technology and we love helping people.

Give me a call today for a quick (non-salesy) chat to find out whether my team and I can help you better secure your data and get more out of your existing technology!

Christopher McManus
Founder & CEO

WHY YOUR EMPLOYEES SHOULDN'T HAVE ADMINISTRATOR ACCESS TO THEIR COMPUTERS

Administrator access can seem like a simple way to solve a problem. An employee needs to install a printer, update a specialized program, or change a setting on their computer. Giving them administrator access gets the job done quickly.

The problem is that the access often stays long after the original request is finished.

Once an employee has administrator privileges, they can approve additional software installations and make system changes that would normally require IT assistance. If they accidentally install the wrong program or their account is compromised, those same permissions can give someone else more control over the computer.

For a small business, that can create an unnecessary security risk.

What administrator access allows someone to do

An administrator has significantly more control over a computer than a standard user. On Windows, members of the local Administrators group have extensive control over that computer and its resources. Microsoft recommends limiting the number of users who have these permissions.

Depending on how the computer is configured and managed, an administrator may be able to:

- Install and remove software
- Add drivers for printers and other equipment
- Create, change, or remove user accounts
- Change important system settings
- Change permissions for files and folders
- Install services that continue running in the background
- Make changes to certain security settings

Mac computers also use standard and administrator accounts. Apple explains that administrators can install and remove software, manage other users, and change system settings. Apple recommends limiting administrative users and using a standard account when administrator access is not needed.

Standard accounts are enough for everyday work

A standard account can still handle the everyday tasks most employees need, including:

- Reading and sending email
- Using a web browser
- Working in Microsoft 365 or Google Workspace
- Accessing approved business applications
- Joining online meetings
- Printing through an installed printer
- Opening and saving files
- Changing personal settings that do not affect other users

Some applications can be installed for an individual user without administrator access. Others require approval because they add drivers, services, or files to protected areas of the computer.

An employee should not receive permanent administrator access simply because one application needs an update.

Instead, IT can approve and install the software, deploy the update remotely, or use a separate administrator account specifically for that task.

How to handle software installations

Employees can still get the software they need without keeping administrator privileges.

Your IT team can install applications remotely, review and approve requests when necessary, or deploy approved updates across multiple computers at once. If a program requires administrator access, your IT provider may also be able to adjust its configuration or identify a supported alternative.

For approved technical work, keep a separate administrator account. Avoid using that account for email, web browsing, or everyday tasks, and protect it with multifactor authentication whenever the system supports it.

Check who has administrator access today

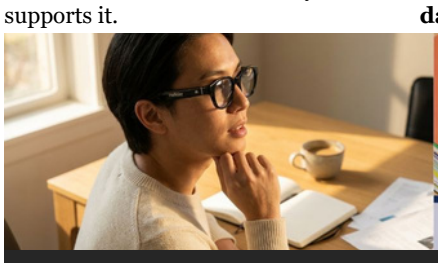
Ask your IT provider to review the administrator accounts on your company computers and systems.

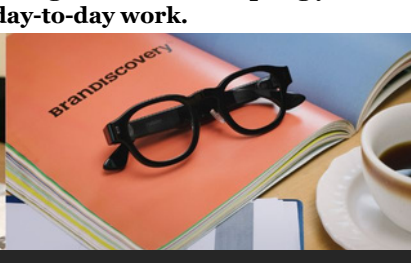
Before removing access, make sure your IT team still has a reliable and tested way to perform administrator level tasks on every device.

Standard user accounts allow employees to get their work done while limiting the amount of control they, and the software they use, have over the computer.

That small change can help reduce unnecessary risk while keeping your team productive.

Need help reviewing your business computers? PowerPro Computers can help you identify where administrator access is being used and make practical changes without disrupting your day-to-day work.





HALLIDAY G2 AI GLASSES

Halliday G2 is a pair of AI powered glasses designed for live meetings, with a heads-up display that shows real-time translations, notes, and prompts in your line of sight. It follows conversations across 45+ languages, tracks decisions and action items, and sends a summary when the meeting ends. A built-in voice assistant handles quick questions hands-free, while a 4-mic array and speakers manage calls and music. With no camera and encrypted data, it is built with privacy at the core.

powerPro computers

SHOULD EMPLOYEES USE PERSONAL DEVICES FOR WORK?

Using a personal phone or computer for work can seem like an easy solution. Employees already know how to use their devices, and they can check email, join a meeting, or handle a quick task without carrying another computer.

But convenience can create questions for your business.

Where is company information being stored? Which applications are employees allowed to use? What happens if the device is lost? And what happens to business information when an employee leaves?

Personal devices can work for limited business tasks when they meet your company's security requirements. For sensitive work, administrative tasks, or situations where large amounts of business information are stored locally, a company-owned device is usually easier to manage and protect.

What counts as a personal device used for work?

Bring Your Own Device, or BYOD, includes more than using a personal phone to check email.

It could mean opening company documents in a mobile app, using a home computer to access a business system, or downloading a work file to a personal device.

That file may remain in a Downloads folder. An employee may also stay signed in to a business account after the work is finished.

These small details can become important when a device is lost, replaced, shared with someone else, or no longer used for work.

Decide what employees can do

Start with the type of work being performed and the information involved.

For example, you might allow employees to check company email through an approved mobile app but require a company computer for payroll, customer database exports, system administration, or access to sensitive client records.

Employees should know which devices and applications are approved, whether they can download company files, and what they need to do before selling, replacing, or giving away a personal device.

Clear rules make BYOD much easier to manage.

Set basic security requirements

If employees are using personal devices for work, those devices should meet some minimum security standards.

Personal devices used for work should meet minimum security standards: an operating system that still receives security updates, a screen lock, encryption where available, and multifactor authentication on company accounts.

Whenever possible, keep business information inside approved applications or a managed work profile rather than allowing company files to spread across the personal device.

Device and application management tools can also help businesses enforce certain security settings and, on supported platforms, remove company information from managed applications.

Employees should understand what the business can access or remove before they enroll a personal device in a company program.

Have a plan for a lost device or departing employee

A lost phone or laptop should not become a scramble to figure out what happens next.

Your IT provider may need to revoke active sessions, reset affected passwords, and remove company information from managed applications.

When an employee leaves, their company accounts should be disabled at the agreed time. Business information should also be returned or removed from the personal device according to your company's policy.

Having this process in place before something happens makes the situation much easier to handle.

When should you provide a company device?

A company-owned computer makes more sense when an employee handles sensitive information, needs administrator access, stores significant business data locally, or uses specialized software.

It is also the better option when your IT team needs greater control over updates, backups, applications, and security settings.

BYOD can work. The key is making sure the convenience does not come at the expense of protecting your business information.

Not sure whether your current BYOD setup is putting your business information at unnecessary risk? PowerPro Computers can help you review your devices, applications, and access rules and recommend practical next steps.

WHAT HAPPENS TO YOUR DATA WHEN YOU CANCEL A CLOUD SERVICE?

Canceling a cloud service may seem simple: stop the subscription and move on.

But what happens to the information stored inside that account?

The answer depends on the provider. Some services may keep your information available for a limited period. Others may restrict access as soon as the subscription ends. Your account could become read-only, remain accessible only to an administrator, or eventually be scheduled for deletion.

That is why it is important to understand the provider's cancellation and data-retention policies before you cancel.

Check the provider's current documentation and your agreement. Confirm when employees will lose access, how long your information will remain available, what your data export includes, and whether you need to request the export while the subscription is still active.

If you purchased the service through a reseller, check the cancellation process with them as well.

Before you cancel, take these steps:

1. Know what is stored there
Make a list of the information your business relies on, including attachments, comments, reports, audit records, customer information, and custom fields.

2. Export and check your data
Do not assume an export is complete just because the download finished.
Open samples of every important file type and check that attachments, dates, customer details, project information, and other important data are still there.

3. Test the move
If you are switching to another service, test the import before the old account closes.
Finding out that important information did not transfer after the old system is gone can create a much bigger problem.

4. Check what connects to the service
Look beyond the main application.
Website forms, payment systems, reports, mobile apps, automated workflows, and other business tools may depend on the account.
Make sure those connections will continue working after the service is canceled.

5. Check account sign-ins
Some employees may use their account with this service to sign in to other applications.
Identify those connections and update the sign-in information before access to the old account disappears.

Do not forget about record-keeping

Your business may need to retain certain financial, customer, employee, or contract records for a specific period.

Those requirements can vary depending on your business and circumstances, so check with the appropriate legal, accounting, or compliance professional before deleting records.

Ask what happens after cancellation

Before closing the account, ask the provider exactly what happens to your information.
Find out what will be deleted from active systems and backups, when deletion will occur, and whether you need to close the account separately after canceling the subscription.

Keep the provider's confirmation with your other business records.

A cloud cancellation should be a planned transition, not a surprise after your data is no longer available.

Thinking about moving away from a cloud service? PowerPro Computers can help you review what needs to be protected, transferred, and checked before you make the switch.

WHY GUEST WI-FI SHOULD BE SEPARATE FROM YOUR BUSINESS NETWORK

Guest Wi-Fi should give visitors internet access without giving their devices a path to your business computers, cameras, file storage, printers, or network equipment.

Simply using a different Wi-Fi name and password does not mean the networks are actually separated. Your router, wireless access points, and firewall need to be configured so guest devices cannot reach systems on your internal business network.

Employee phones, personal laptops, and other devices that only need internet access can normally use the guest network instead of connecting directly to your business network.

This can be especially helpful in offices where clients, vendors, visitors, or contractors regularly need Wi-Fi access.

Ask your IT provider to test the guest network and confirm that connected devices can access the internet but cannot open internal systems, shared files, cameras, printers, or network management pages.

Most small businesses do not need a separate internet connection to accomplish this. One internet connection can support both employee and guest Wi-Fi while keeping the networks properly separated.

A properly configured guest network gives visitors the connectivity they need while helping keep your business systems where they belong: accessible to the people who need them, and separated from everyone else.

SMALL BUSINESS IT BUDGET: WHAT TO INCLUDE AND HOW TO PLAN IT

An IT budget should reflect the technology your business relies on today and the changes you expect during the year. Start with an inventory of computers, network equipment, software, cloud services, phone systems, websites, domains, backups, and IT support contracts.

Separate regular operating costs from one time purchases and larger technology projects. Include employee onboarding and offboarding, staff training, backup testing, cybersecurity reviews, and equipment disposal.

It is also smart to keep a reserve for an urgent computer replacement, unexpected equipment failure, or work that falls outside your normal support agreement.

Review your budget every quarter and compare it with your actual invoices. Look for unused software licenses, new subscriptions, price changes, and projects that are costing more than expected.

A good IT budget is not just about controlling costs. It helps you plan ahead, avoid surprises, and make sure your technology supports the way your business operates.

Need help reviewing your technology costs? PowerPro Computers can help you identify what to plan for and where your IT budget may need attention.

HOW LONG BUSINESS COMPUTERS LAST AND WHEN TO REPLACE THEM

Three to five years is a practical replacement range for many business computers, but age alone should not make the decision. Start reviewing each computer around the three-year mark, then look at its security support, reliability, performance, warranty, and repair history.

Security should come first. Replace a computer if it cannot run an operating system that still receives security updates or support the software your business needs.

A computer that works well can still need replacing if its operating system is no longer supported.

Keeping an outdated system in daily business use can create unnecessary security and compatibility concerns.

Before an older computer is sold, donated, recycled, or returned, make sure important business data has been transferred and the storage drive has been properly erased.

It also helps to keep a simple replacement schedule for every computer. Record the purchase date, assigned user, warranty expiration, operating system, and next review date.

Ask your IT provider to review your business computers at least once a year. A regular review can help you spot aging equipment before it becomes an unexpected problem.

If you do not have an IT provider, PowerPro Computers can help you review your current equipment and plan replacements around your business needs and budget.

TECHNOLOGY TRIVIA TIME

Each month, you have a chance to win a $50 Amazon gift card by answering our Technology Trivia Question of the Month!

TAKE THE QUIZ & WIN

Click below to answer this month's Technology Trivia question and enter for your chance to win.

Click Here

LAST MONTH'S ANSWER
Image Maximum