

TECH TALK

M O N T H L Y



Why Your Employees Shouldn't Have Administrator Access to Their Computers

Inside:

- ✓ Should Employees Use Personal Devices for Work?
- ✓ What Happens to Your Data When You Cancel a Cloud Service?
- ✓ Why Guest Wi-Fi Should Be Separate From Your Business Network
- ✓ Small Business IT Budget: What to Include and How to Plan It
- ✓ How Long Business Computers Last and When to Replace Them

What's Inside

Page 1:

- **Why Your Employees Shouldn't Have Administrator Access to Their Computers**

Page 2:

- **Should Employees Use Personal Devices for Work?**

Page 3:

- **What Happens to Your Data When You Cancel a Cloud Service?**

Page 4:

- **Why Guest Wi-Fi Should Be Separate From Your Business Network**

Page 5:

- **Small Business IT Budget: What to Include and How to Plan It**

Page 6:

- **How Long Business Computers Last and When to Replace Them**

Dear Fellow Business Owner 🙌

An employee needs software installed, so they're given administrator access. A visitor asks for Wi-Fi, so someone shares the office password. Staff start using personal phones for work, but nobody agrees on what they may access or where company files may be stored.

Those decisions solve an immediate problem, but they can leave you with more access than people need, business information on devices you don't control, and systems that are difficult to manage when someone leaves.

This month, we explain why employees should use standard computer accounts, how to set rules for personal devices, and what to do before canceling cloud software. We also cover guest Wi-Fi, IT budgeting, and when an older computer should be repaired or replaced.

Check whether your current setup still matches the way your team works. If visitors have used the same Wi-Fi password for years, ask your IT provider to check the network. If employees use personal devices, make sure the rules are written down. And if several computers are reaching three or four years old, add their likely replacement dates to next year's budget.

If you'd like help checking any of these areas, give us a call.

Stay safe,



Tony Loffi-Lara
CTO, Oasis Technologies

DID YOU KNOW ?

The first computer mouse was made from redwood in 1964. The team called it a mouse because its cable made it look like one with a tail.

GET IN TOUCH

- 📞 405.996.7124
- 🌐 oasis.tech/tony
- ✉️ tlara@oasis.tech

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

Administrator access often starts with a reasonable request. Someone needs to install a printer, update a program, or change a setting, so they're made an administrator on their computer. The task gets done, but the access stays.

From then on, that employee can approve software installations and make changes that normally require help from IT. If they download a fake installer or approve a harmful program, it may be able to install system components, change security settings, or affect other information on the computer.

For email, web browsing, documents, meetings, and most business applications, employees should use standard accounts. Administrator access should be reserved for approved IT work.

What administrator access allows

On Windows, members of the local Administrators group have broad control over that computer. They may be able to install software, add drivers, manage other local users, and change system settings or file permissions. Mac computers also have standard and administrator accounts, with similar differences in what each can change.

Why standard accounts are safer

Programs normally start with the permissions available to the person who launches them. If an employee can approve an administrator request on their own, harmful software may receive the same level of access.

Windows uses User Account Control to ask before many important changes. An employee using an administrator account can approve that request. A standard user is normally asked for administrator credentials, which gives IT an opportunity to check the program and where it came from.

Standard accounts still support normal work. Employees can use email, browsers, Microsoft 365 or Google Workspace, meetings, approved software, printers, and shared files.



How to handle software installations

Employees can still get software installed without keeping administrator access. Your IT team can install it remotely, approve a request when it is needed, or deploy updates to several computers at once.

Test specialist or older software before changing permissions across the business. If a program expects the user to be an administrator, your IT provider may be able to change its setup or find a supported alternative.

Keep a separate administrator account for approved technical work. Do not use it for email, web browsing, or everyday tasks, and protect it with multifactor authentication where the system supports it.

Check who has access now

Ask your IT provider to review the administrator accounts on every company computer, including former employees, shared logins, vendor accounts, and accounts created during the original setup.

Before removing access, confirm that IT still has a tested way to perform administrator tasks on every device.

Standard accounts let employees do their jobs without giving them or the software they run more control than normal work requires.

SHOULD EMPLOYEES USE PERSONAL DEVICES FOR WORK?

Allowing employees to use personal phones or computers can be convenient. They already know the device, and they can check email or join a meeting without carrying another piece of equipment.

But the business still needs to decide what work is allowed, which applications employees may use, and what happens to company information if a device is lost or an employee leaves.

Personal devices can be suitable for limited work when they meet your security requirements. Company-owned devices are a better choice for sensitive work, administration, or jobs that require large amounts of business data to be stored on the device.



What counts as a personal device used for work?

Bring your own device, often shortened to BYOD, includes reading company email on a personal phone, opening documents in mobile apps, or using a home computer to connect to a business system. Files may remain in the Downloads folder, and accounts can stay signed in after the work is finished.

Decide what employees may do

Set the rules according to the work and the information involved. You might allow employees to read email through an approved mobile app but require a company computer for customer database exports, payroll, system administration, or access to sensitive client records.

Staff should know which devices and applications are permitted, whether they may download files, and what they must do before selling or replacing the device.

Set minimum security requirements

A personal device should run an operating system that still receives security updates. It should have a screen lock, device encryption where available, current updates, and

multifactor authentication on company accounts. A lost or stolen device must be reported quickly.

Keep business information inside approved applications or a managed work profile where possible. Device and app management tools can apply security settings and, on supported platforms, remove company data from managed apps. Tell employees what the business can see or remove before they enroll their device.

Plan for a lost device or departing employee

If a personal device is lost, IT may need to revoke active sessions, reset affected passwords, and remove company information from managed apps.

When an employee leaves, disable their account and active sessions at the agreed time. Remove company data from managed apps, check for downloaded files, and confirm that business information has been returned or deleted.

When to provide a company device

Use a company-owned device when an employee handles sensitive information, needs administrator access, stores a large amount of data locally, or requires specialist software. It is also the better choice when IT needs full control over updates, backups, applications, and security monitoring.

BYOD can work, but only when the rules are clear and the device can meet them. If your business allows personal devices, ask your IT provider to review the policy, access settings, and offboarding process before a lost phone or employee departure puts company data at risk.

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

Every cloud provider handles cancellations differently. One may leave your information available for a limited time, while another may restrict access as soon as the subscription ends. An account may become read-only, remain available only to an administrator, or be scheduled for deletion.

Check the provider's current documentation and your contract before canceling. Confirm when employees will lose access, how long the data will remain available, what the export contains, and whether you must request it while the subscription is active. If you bought the service through a reseller, check the cancellation process with the reseller as well.

Before you cancel:

1. List the information stored in the service, including attachments, comments, reports, audit records, and custom fields.
2. Export what the business needs and open a sample of every file type. Make sure attachments, dates, and customer or project details are complete.
3. If you are moving to another service, test the import before the old account closes.
4. Check website forms, payment tools, reports, mobile apps, automated workflows, and other systems connected to the service.
5. Confirm whether employees use the account to sign in to another application, then change those sign-ins first.

Your business may need to keep financial, customer, employee, or contract records for a set period. Check those requirements with the appropriate legal, accounting, or compliance adviser.

Ask the provider what it will delete from active systems and backups, when deletion will take place, and whether you need to close the account separately after canceling the subscription. Keep the confirmation with your other business records.



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

Guest Wi-Fi should give visitors internet access without allowing their phones or laptops to connect to your business computers, printers, cameras, file storage, or network equipment.

A different Wi-Fi name and password do not prove that the networks are separated. The router, wireless access points, and firewall must be configured so guest devices cannot reach the internal network. Guest devices should usually be blocked from connecting to one another as well.

Employee phones and personal laptops that only need internet access can

normally use the guest network.

Connected devices such as smart TVs and cameras may need their own separate network.

Ask your IT provider to test the guest Wi-Fi and confirm that it can reach the internet but cannot open internal systems or management pages. Most small businesses can use one internet connection while keeping these networks separate.

Keep the guest password different from the business Wi-Fi password, and change it when needed.



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

An IT budget should reflect the systems your business uses and the changes expected during the year. A general percentage of revenue cannot tell you whether you have allowed enough for a new employee, a failed laptop, or a software renewal.

Start with an inventory of computers, network equipment, software, cloud services, phone systems, websites, domains, backups, and support contracts. Record the cost, renewal date, contract owner, notice period, and number of licenses for each service.

Separate normal running costs from one-time purchases and projects. Recurring

costs include software, IT support, internet, phones, backup, and security tools. One-time costs include new equipment, migrations, installations, office moves, and major upgrades.

Include onboarding and offboarding, staff training, backup testing, cybersecurity reviews, and equipment disposal. Keep a reserve for an urgent replacement or work outside a support agreement.

Review the budget every quarter against actual invoices. Check for unused licenses, new subscriptions, price changes, and projects that are costing more than expected.



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 decide it. Start reviewing each device at three years, then check its security support, reliability, performance, warranty, and repair history.

Security comes first. Replace a computer if it cannot run an operating system that still receives security updates or the software your business requires. A computer that still runs well may need replacing if its operating system is no longer supported.

Have a slow computer checked before replacing it. Low storage, insufficient memory, overheating, malware, or an operating-system problem can all affect performance. An upgrade may be worthwhile if the computer remains supported and reliable.

Keep a replacement schedule with the purchase date, assigned user, warranty expiry, operating system, and review date for every computer. This lets you spread purchases across several budget periods.



Before an old computer is sold, donated, recycled, or returned, transfer the required data and have its storage properly erased. Deleting files or removing an account does not guarantee that the information is gone.

Ask your IT provider to review your computers at least once a year. If you do not have an IT provider, feel free to reach out to us and we'll help you plan the replacements.

Thank You!

Thanks for taking the time to read this month's newsletter. We hope you picked up a few helpful tips or ideas to make your tech work a little smarter for you.

If you ever have questions, or just want a second opinion on anything IT-related, we're only a phone call or email away.

CONTACT US BELOW



405.948.6500



info@oasis.tech



oasis.tech



**6317 NW 23rd St.
Bethany, OK 73008**

