IT Department

March 2026

NewsLetter

Work Order System \ Spring Cleaning Your Digital World

Identity Theft \ Don't Click Random Links \ Identity Theft: What's New
The Floating Computer Desk

Why A Work Order System Matters

When something breaks, it's easy to walk down the hall, send a quick email, or tell someone directly. That feels efficient in the moment. But at an organizational level, it is not sustainable. If we are serious about service, accountability, compliance, and long term improvement, we cannot rely on memory or scattered conversations. We need structure. That is what a Work Order system provides.

A Work Order system is our organizational memory. It answers the essential questions: What was the problem? What caused it? Who or what did it affect? What was done to resolve it? And how do we prevent it from happening again? Without documentation, those answers fade. Months or years later, when someone asks why a configuration was changed, why a device was replaced, or why an individual was granted certain permissions, "I think" or "I remember" is not sufficient. A documented record gives us clarity when memory no longer serves.

Simply telling someone about an issue leaves no audit trail, no measurable history, and no way to analyze patterns. An electronic Work Order creates a time stamped, traceable record. It documents who initiated the request, what actions were taken, and how it was resolved. In regulated environments, that matters. If we need to review why access was granted, who approved a change, or whether an exception was justified, the Work Order becomes the record of rationale. IT executes actions, HR determines employment status, departments define access needs : the Work Order captures the coordination between them.

Beyond compliance, tracking allows us to move from reactive to proactive service. When issues are documented consistently, we can see trends. Are password resets increasing? Is a specific location experiencing repeated equipment failures? Is a system generating unnecessary friction? Data reveals patterns. Patterns allow prevention. The goal is not simply to close tickets; it is to reduce recurring problems and improve service delivery across the agency.

Electronic tracking is best practice because it centralizes intake, standardizes prioritization, preserves communication, and enables reporting and secure archiving. It removes guesswork and creates transparency. Our new Work Order system enhances visibility, tracking, and reporting functionality so we can serve you more effectively. But systems must serve people. Let me ask the question, when it comes to work orders and IT, what information would help you most, what could be clearer, and how can we refine this process to better support your work? Let someone in the IT department know and they will pass that on to me, or send me an email directly : jeff@saratogabridges.org.

If you experience issues or have suggestions regarding the new system, please contact Tech Support at

587-0723 ext. 1333

For after-hours and weekend support, call 518-450-9024.

For Relias password issues during business hours, contact the Training Department.

A Work Order system is not bureaucracy. It is discipline. It protects the agency, the staff, and the individuals we serve. Most importantly, it allows us to improve; not just today, but continuously.

Spring Cleaning Your Digital World

As we move into March and the start of spring, many of us begin thinking about cleaning and organizing our homes. But what about our digital spaces? Just like closets and garages, our devices and online accounts can accumulate clutter over time. This month, the IT Department is focusing on “Digital Spring Cleaning” — simple steps everyone can take to stay secure, organized, and productive.

1. Update Your Devices

One of the easiest and most important things you can do is keep your devices up to date. Whether it’s your smartphone, tablet, laptop, or desktop computer, software updates often include security improvements that protect you from new threats.

If you see a notification to update your system or apps, don’t ignore it. Set your devices to update automatically if possible. These updates are designed to fix weaknesses that cybercriminals actively look for.

2. Review Your Passwords

March is a great time to review your passwords. Weak or reused passwords are one of the most common causes of online security issues.

Here are a few quick tips:

- Use a unique password for each important account.
- Make passwords long and hard to guess (a short sentence can work well).
- Consider using a password manager to keep track of them securely.
- Turn on multi-factor authentication (MFA) when available. This adds an extra layer of protection by requiring a second form of verification, such as a code sent to your phone.

3. Clean Up Your Inbox

Email inboxes can quickly become overwhelming. Unsubscribe from newsletters you no longer read and delete old messages that are no longer needed. Be cautious when opening attachments or clicking links, especially if the message feels urgent or unexpected.

If you receive a suspicious email:

- Do not click on links.
- Do not download attachments.
- Report it using your organization's reporting process or delete it.

Phishing emails are designed to look real, so when in doubt, verify through a trusted contact method.

4. Back Up Important Data

Think about the photos, documents, and important files stored on your devices. If your device were lost, damaged, or infected with malware, would you still have access to them?

Backing up your data ensures you have a copy in a secure location. This can be done using:

- An external hard drive.
- A secure cloud storage service.
- Automatic backup tools built into your device.

Regular backups provide peace of mind and reduce the risk of permanent data loss.

5. Organize Your Files

Take a few minutes to review your desktop and file folders. Create clearly labeled folders for important documents and remove duplicates or outdated files. An organized system makes it easier to find what you need and improves overall productivity.

You might also consider reviewing apps on your phone or computer. Delete applications you no longer use. Fewer apps mean fewer potential security risks and better device performance.

Spring is about fresh starts. By taking small steps to clean and secure your digital life, you can reduce risks and improve efficiency. The IT Department is here to support you with guidance, tools, and answers to your questions.

If you need assistance with updates, password management, backups, or identifying suspicious activity, please reach out. A safer digital environment starts with simple, proactive habits — and March is the perfect time to begin.

---

says the Sticker

Save the !'s

Nothing is as motivating as when our co-workers let us know they appreciate us. We're social animals and the regard of our fellow creatures feels good. Good tends to beget good so we find it to be to our advantage to thank people when they do something for us. We'll send an email to a co-worker letting them know we're done with some routine tasks they asked us to do and we get a reply from them that says "Thanks!". While the acknowledgement is appreciated, they did say thank-you, after all, one can wonder if their apparent enthusiasm is proportionate to the imposition caused by completing the task. If the task was a routine part of our job, and we completed it withing the expected timeframe at the standard level of quality, then the enthusiasm conveyed by the "!" in "Thanks!" may be a bit overblown…..or the punctuation mark is being used to convey a different meaning.

Identity Theft: What's New and How to Stay Safe

Hello and Welcome

Identity theft is when someone steals your personal information and pretends to be you. This can include your name, Social Security number, passwords, or bank details. Criminals are always finding new tricks. These are only a few of the newest ones and how to prevent them.

New Tricks Criminals Are Using

1. **Fake Text Messages (Smishing)**

You may get a text that says your package is delayed or your bank account is locked. It asks you to click a link. The link takes you to a fake website that steals your information.

2. **Fake Phone Calls (Vishing)**

Someone calls and says they are from IT, your bank, or even your supervisor. They may sound real and even know your name. They will ask for passwords or a code sent to your phone.

3. **Email Account Takeovers**

Criminals send emails that look like they are from companies like Microsoft or Amazon or even worse, NETFLIX. If you click and sign in, they steal your password.

4. **Social Media Scams**

Fake profiles pretend to be friends or coworkers. They may ask for gift cards or personal details.

How to Protect Yourself

- **Do not click links in unexpected texts or emails.**

If you are unsure, go directly to the company's website instead.

- **Never share your password or security codes**.

The Saratoga Bridges IT staff will NEVER ask for your password.

- **Turn on Multi-Factor Authentication (MFA) for bank accounts and any other site that has this option available.**

This adds a second step when logging in, like a code on your phone.

- **Use strong, different passwords.**

A password manager can help you remember them.

- **Slow down.**

How to Protect Your Family, Friends, and Co-workers

- **Alert your intended receiver that you will be sending them an email that has a Weblink to a site or that it has an attachment ahead of time. You may even want to pick up the phone and call them directly prior to send that all too important email.**
- **Never forward emails that have interesting jokes or attachments that come from unknown sources**
- **Never forward emails that are questionable to the IT department asking, "Is this a virus?"**

Scammers want you to panic. Take a breath before you click.

Did You Know? 

In 2024, a major health care company called Change Healthcare was hit by a large cyberattack. Criminals broke into their systems and caused delays in payments and services across the country. Many hospitals and providers were affected.

This shows that even big companies can be targets. That's why it's important for all of us to stay alert and follow safe online habits every day.

Microsoft Outlook Safety Tip: Check Before You Click

👉 **Hover your mouse over a link before clicking.**

When you move your mouse over a link (without clicking), you can see the real web address. If the address looks strange or misspelled, do not click it.

Also:

- **Look for spelling mistakes in the email.**
- **Be careful if the message says "urgent" or asks for gift cards.**
- **Use the "Report Phishing" button if you are unsure.**

Taking a few extra seconds can prevent big problems.

If You Think Something Is Wrong

Report it right away to the IT Department. Acting fast can help stop damage before it spreads.

Staying safe online protects you, your coworkers, and the people we support. Thank you for helping keep Saratoga Bridges secure!

Please don't forget to change your passwords and make sure that they are complex enough that no one can guess them. Think Spring!

🚫 **IT Tips: What *Not* To Do**

❌ **Don't Click Random Links**

Phishing is the most common cyberattack, and it's getting more convincing every year. Before you click anything, take a moment to check:

- **Sender's real email address**
- **Unexpected attachments**
- **Urgent or threatening language ("Your account will be closed!")**
- **Links that look suspicious or misspelled**

When in doubt, ask IT before opening the message.
It's always better to double-check than deal with a compromised account.

🌨️ **Stay Warm**

Cold weather doesn't just affect people—it affects technology too.

Protect Your Devices from the Cold

- **Don't leave laptops or phones in cold cars; when they warm up too fast, condensation can damage internal components.**
- **Always let devices return to room temperature before powering them on.**
- **If you're commuting, keep electronics in an inside coat pocket or an insulated bag.**

A little temperature awareness can save your devices from a frosty fate.

🎉 **Just for Fun — March Tech Riddle**

Riddle:
I have keys but no locks. I have space but no room. You can enter, but you can't go outside. What am I?

Answer:
Your keyboard — where dreams, productivity, and the occasional typo are brought to life.

The Floating Computer Desk for Offices and Residential home.

Keeping your desk clean and organized is something the IT Department looks forward to seeing. We would like all office desks to be just like this, especially when we have to install hardware or other components to your desktop and your area is well kept. Sometimes the IT Department needs to run some Network lines behind your desk and the wall which can be a very very interesting journey into that " Unknown World" filled with Magical missing pens, mystical paper clips and those Post-It-Notes that strangely went missing plus all the other items you lost from Long Long Ago falling into the Abyss, yes, you know that Dark Cave behind your desk and the wall. I will say this only seems to affect offices and residential houses with computer desks. This will standardize all desks for everyone across all offices and residential houses. No need to purchase anymore desks as these can be built on campus, much less then the cost of desk every few years.

“But Phil, can you really help all the Desktopians and bring Peace to this Campus?

‘Well I am sure can help resolve this issue and make the Desktopians happy again.

Here in the IT Department, we have a system of Wall Desks which are built into the wall and can provide much more space over computer desks. Have you noticed the “Cubi-topians” they have these Floating Wall Desk and you can see they have much more room, including space under the Wall Desk for anything, like file cabinets, storage, foot warmer and mini frigs. Best of all IT has more room to run those IT Network lines or connect printers and scanners. We can also add a Wire Management system, so you don’t have all those wires near your feet. No more tangled twisted wires, much easier access for the IT Department.

Bottom Line - More space and more space mean better organization, easier access for the IT Department for everything you need like your office phones, cell phones and charging area for all your USB needs. The Wall Desk can provide more room for your printer, scanner and other devices. This will also end the ability to move anything anything in IT. This is just a concept at this point, and I welcome all your feedback on this idea of Wall Desk. I will have more to say about this in future Newsletters.

Send comments to: Editor - Phil Ellsworth pellsworth@saratogabridges.org