ATTITUDE IT
Keeping Your Technology On Course

BEYOND CHATBOTS: PREPARING YOUR SMALL BUSINESS FOR "AGENTIC AI" IN 2026

AI chatbots can answer questions. But now picture an AI that goes further, updating your CRM, booking appointments, and sending emails automatically. This isn't some far-off future. It's where things are headed in 2026 and beyond, as AI shifts from reactive to proactive, autonomous agents.

This next wave of AI is called "Agentic AI." It describes AI that can set a goal, figure out the steps, use the right tools, and get the job done on its own. For a small business, that could mean an AI that takes an invoice from inbox to paid, or one that runs your whole social media presence. The upside is massive efficiency, but it also means you need to be prepared. When AI gets more powerful, having the right controls matter.

What Makes an AI "Agentic"?

A research article on the evolution and architecture of AI agents explains the big shift like this: AI is moving from tools that wait for instructions to systems that work toward goals on their own. Instead of just helping with tasks, AI starts doing the work, making it possible to hand off whole processes and collaborate with it like a teammate.

The 2026 Opportunity for Your Business

For small businesses, this is about real leverage. Agentic AI can work around the clock, clear out repetitive bottlenecks, and cut down errors in routine processes. That means things like personalizing customer experiences at scale or even adjusting supply chains in real time become possible.

And this isn't about replacing your team. It's about leveling them up. AI takes the busywork so your people can focus on strategy, creativity, tough problems, and relationships, the things humans do best. Your role shifts too, from doing everything yourself to guiding and supervising your AI.

What You Need Before You Launch Agentic AI

Before you hand over your processes to an AI agent, you need to make sure those processes are rock solid. The reasoning is simple: AI will amplify whatever it touches, order or chaos, with equal efficiency. That's why preparation is key. Start with this checklist:

1. **Clean and Organize Your Data:** AI agents make decisions based on the data you give them. Garbage in means not just garbage out; it can lead to major errors. Audit your critical sources.
2. **Document Workflows Clearly:** If a human can't follow a process step by step, an AI won't be able to either. Map out each workflow in detail before you

Building Your Governance Framework

Just like with human team members, delegating to an AI agent requires oversight. That means setting up clear guardrails by asking a few key questions:

- What decisions can the AI agent make on its own?
- When does it need human approval or guidance?
- What are its spending limits if it handles finances?
- Which data sources is it allowed to access?

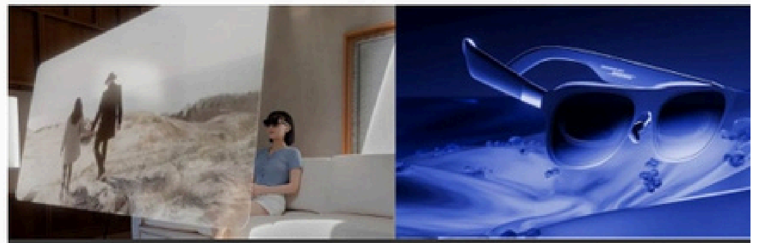
Answering these questions lets you build a framework that becomes your company's rulebook for its "digital employees."

Security is another critical piece. Every AI agent needs strict access controls, following the principle of least privilege. Regular audits of agent activity are now a non-negotiable part of good IT hygiene.

Embracing the Role of Strategic Supervisor

Agentic AI is a true force multiplier, but it depends on clean data and well-defined processes. It rewards careful preparation and punishes the hasty. By focusing on data integrity and process clarity now, you position your business not just to adapt, but to lead.

Contact us today for a technology consultation on AI integration. We can help you audit workflows and create a roadmap for reliable, effective adoption.



XREAL 1S AR GLASSES

XREAL 1S packs a stunning micro-OLED display, a wider 52-degree field of view, and crisp 1200p resolution into a comfortable, sunglasses-style frame built for everyday use.

With plug-and-play support for phones, laptops, consoles, and handheld gaming devices, you can enjoy a massive virtual screen anywhere. It delivers smooth 120Hz visuals, Bose-tuned speakers, and simple on-device controls, making it effortless to switch between gaming, streaming, or productivity on the go.

ATTITUDE CHRONICLE

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

The "Insider Threat" You Overlooked: PROPER EMPLOYEE OFFBOARDING

When an employee leaves your company, their access does not automatically disappear.

For many Ontario businesses, employee offboarding is handled casually. Collect the laptop, say goodbye, and move on. But what often gets missed is the digital access that remains active long after someone walks out the door.

That gap creates serious cybersecurity and compliance risk. A former employee whose email still works, whose login credentials remain active, or who can still access cloud storage and project systems represents a real vulnerability. Sometimes the risk is malicious. More often, it is simple oversight.

Either way, the consequences can be costly.

For construction companies, that could mean access to project files, drawings, and financial data. For manufacturers, it could mean access to production systems, supplier lists, or inventory platforms. For professional firms, it could mean exposure of client records and confidential communications. Offboarding is not administrative paperwork. It is a critical layer of business protection.

The Hidden Risk of a Casual Goodbye

A handshake and returned laptop are not enough.

Today's employees accumulate digital access across multiple platforms including email accounts, accounting systems, cloud storage, project management tools, remote access portals, vendor systems, and internal servers.

Without a formal IT offboarding process, it is almost guaranteed that something will be missed.

Old accounts are prime targets for cybercriminals.

If login credentials are reused elsewhere and exposed in a breach, attackers may gain trusted access to your systems without triggering alarms. In Ontario's regulatory environment, this can also create compliance exposure under privacy laws and industry regulations.
The risk is not theoretical. It is operational.

Why Offboarding Is a Cybersecurity Control — Not Just an HR Task

A proper IT offboarding process should be immediate, documented, repeatable, and coordinated between HR and your IT provider. Access must be removed systematically for every departure, whether the employee resigned, was terminated, or retired.

The first step is maintaining a clear inventory of all user accounts, software platforms, issued devices, shared credentials, and remote access permissions.

Without visibility into what an employee has access to, security gaps form quickly.

What a Strong Employee Offboarding Process Looks Like

A secure offboarding process begins the moment notice is given. Primary access such as email accounts, network logins, remote access, and cloud platforms should be disabled immediately upon departure.

Shared passwords for social media accounts, departmental inboxes, and vendor portals should be reset to prevent continued access.

All company-issued devices including laptops, tablets, and mobile phones should be collected promptly. Before reissuing those devices, company data should be securely removed to prevent residual access.

Cloud documents, shared files, and project ownership must be transferred to appropriate team members to ensure business continuity.

continues on page 2.....

It is also important to review recent access activity prior to departure to confirm that sensitive customer data, financial records, or proprietary information were not downloaded unnecessarily.

Finally, software licenses and subscriptions should be cancelled or reassigned to prevent ongoing billing for former employees.

These steps may sound simple, but without documentation and accountability, they are often inconsistently applied.

The Financial and Legal Impact of Poor Offboarding

Weak offboarding processes can result in data theft, ransomware exposure, deleted or altered files, client list extraction, and compliance violations. Even accidental data retention in personal accounts can create regulatory issues and insurance complications.

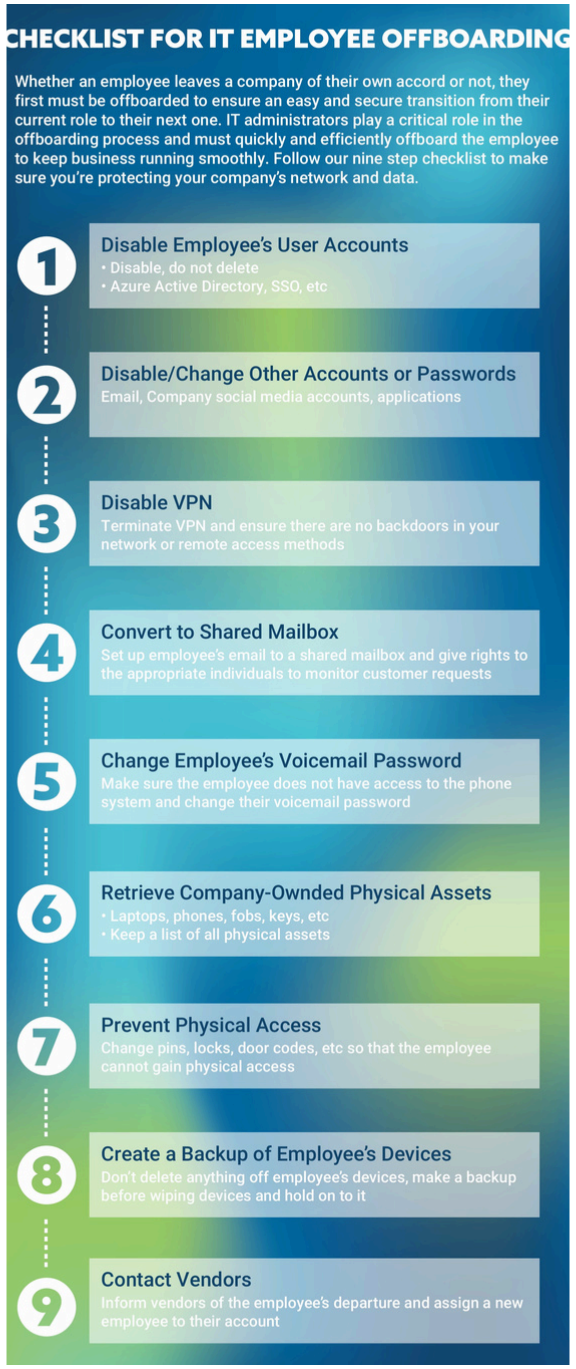
There is also a financial impact that many Ontario business owners overlook. Software subscriptions may continue billing long after an employee has left. Over time, this unnecessary spending adds up and reflects weak internal controls.

For construction and manufacturing companies operating on tight margins, even minor disruptions or preventable expenses can impact profitability.

Strong governance protects both security and the bottom line.

Building a Culture of Secure Transitions

Secure offboarding should be embedded into company policy from day one. Employees should understand that system access is tied to employment and will be removed when they leave. Every departure should follow a documented and consistent process that creates an audit trail and reduces liability.



CHECKLIST FOR IT EMPLOYEE OFFBOARDING

Whether an employee leaves a company of their own accord or not, they first must be offboarded to ensure an easy and secure transition from their current role to their next one. IT administrators play a critical role in the offboarding process and must quickly and efficiently offboard the employee to keep business running smoothly. Follow our nine step checklist to make sure you're protecting your company's network and data.

1. Disable Employee's User Accounts
   - Disable, do not delete
   - Azure Active Directory, SSO, etc
2. Disable/Change Other Accounts or Passwords
   Email, Company social media accounts, applications
3. Disable VPN
   Terminate VPN and ensure there are no backdoors in your network or remote access methods
4. Convert to Shared Mailbox
   Set up employee's email to a shared mailbox and give rights to the appropriate individuals to monitor customer requests
5. Change Employee's Voicemail Password
   Make sure the employee does not have access to the phone system and change their voicemail password
6. Retrieve Company-Ownded Physical Assets
   - Laptops, phones, fobs, keys, etc
   - Keep a list of all physical assets
7. Prevent Physical Access
   Change pins, locks, door codes, etc so that the employee cannot gain physical access
8. Create a Backup of Employee's Devices
   Don't delete anything off employee's devices, make a backup before wiping devices and hold on to it
9. Contact Vendors
   Inform vendors of the employee's departure and assign a new employee to their account

As your organization grows, a structured and potentially automated offboarding process becomes even more important to maintain control and compliance.

Turn Employee Departures into a Security Strength

Every employee departure presents an opportunity to review access permissions, remove outdated accounts, clean up unused software, and strengthen internal controls.

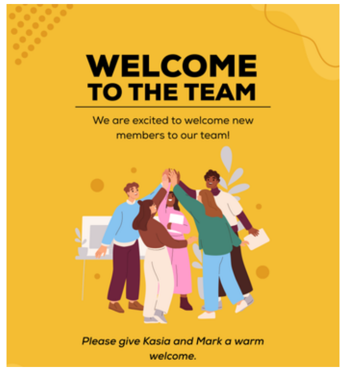
Instead of treating offboarding as a simple administrative task, Ontario business owners should view it as a routine cybersecurity checkpoint. Organizations that take offboarding seriously reduce insider threats, strengthen compliance, protect sensitive data, and preserve their reputation.

Protect Your Business Before the Next Departure

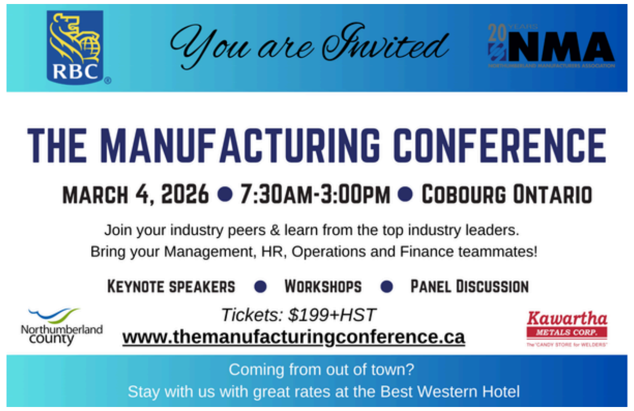
If your organization does not have a documented IT offboarding process in place, now is the time to implement one.

At Attitude IT, we help Ontario construction companies, manufacturers, and professional firms build structured, secure offboarding workflows that protect business-critical systems and reduce compliance risk.

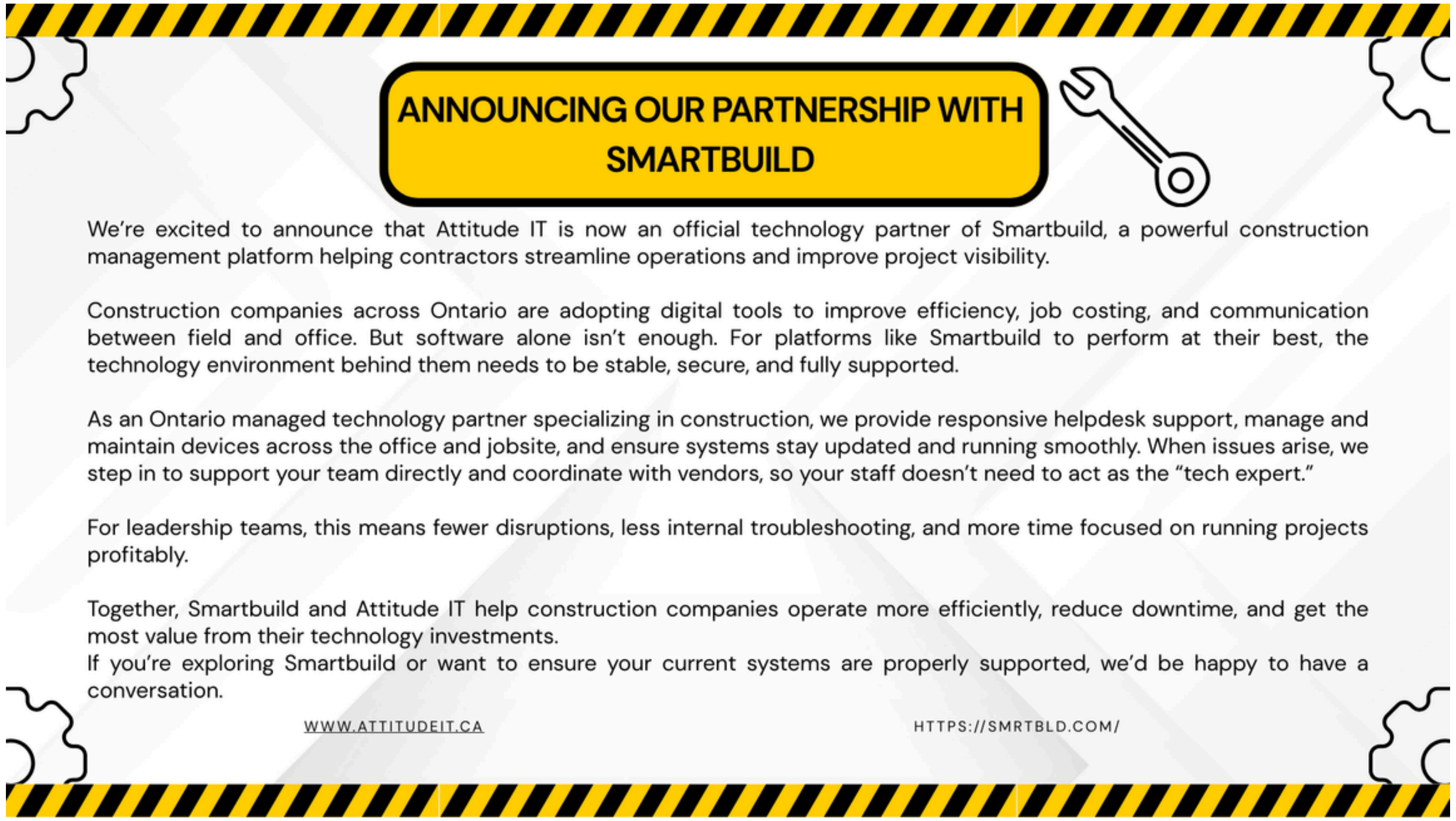
Don't let former employees linger in your digital environment.
Set up a consultation to review your current offboarding process and ensure your business remains protected — even after someone leaves.


WELCOME
TO THE TEAM
We are excited to welcome new members to our team!
Please give Kasia and Mark a warm welcome.

Partnership Announcement
smartbuild™ Powered With Microsoft
&
ATTITUDE IT
Keeping Your Technology On Course
HTTPS://SMRTBLD.COM/
HTTPS://WWW.ATTITUDEIT.CA/



RBC
NMA
Northumberland County
Kawartha METALS CORP.



ANNOUNCING OUR PARTNERSHIP WITH SMARTBUILD

We're excited to announce that Attitude IT is now an official technology partner of Smartbuild, a powerful construction management platform helping contractors streamline operations and improve project visibility.

Construction companies across Ontario are adopting digital tools to improve efficiency, job costing, and communication between field and office. But software alone isn't enough. For platforms like Smartbuild to perform at their best, the technology environment behind them needs to be stable, secure, and fully supported.

As an Ontario managed technology partner specializing in construction, we provide responsive helpdesk support, manage and maintain devices across the office and jobsite, and ensure systems stay updated and running smoothly. When issues arise, we step in to support your team directly and coordinate with vendors, so your staff doesn't need to act as the "tech expert."

For leadership teams, this means fewer disruptions, less internal troubleshooting, and more time focused on running projects profitably.

Together, Smartbuild and Attitude IT help construction companies operate more efficiently, reduce downtime, and get the most value from their technology investments.
If you're exploring Smartbuild or want to ensure your current systems are properly supported, we'd be happy to have a conversation.

WWW.ATTITUDEIT.CA HTTPS://SMRTBLD.COM/

CYBER
BREWS
BEER · FOOD · NETWORKING
SAVE THE DATE
March 12, 2026
RSVP to attend Call 905-432-7751 or
email info@attitudeit.ca

JOINT WEBINAR
SMARTBUILD AND ATTIUDE IT
SAVE THE DATE: MARCH26TH 3:00PM
TO RESEVE A SPOT CALL 905-431-7751
OR EMAIL INFO@ATTITUDEIT.CA