MICROSOFT DYNAMICS GP FINANCIAL SYSTEMS AND ERP IT AND SECURITY

Don't risk your financial data: Security reminders for Dynamics GP

BY PROFESSIONAL ADVANTAGE - 22 July 2025 - 5 MINS READ

Any time is an ideal time to revisit your Microsoft Dynamics GP security. Even whilst you are mapping out a transition, your financial data remains a prime target for cyber threats—and your Dynamics GP environment demands continual attention to stay secure.

If it's been a while since you reviewed your security settings, updated access permissions, or tested backups, consider this your reminder: **now's the time.**

As you plan your migration from Dynamics GP, discover more about the journey to Dynamics 365 Business Central *here*.

Why Dynamics GP security still deserves your attention

Financial systems remain among the most frequently targeted by cybercriminals. And while Dynamics GP has solid security capabilities, they only work if they're correctly configured, maintained, and reviewed regularly.

Five areas you should check right now:

1. User access: Who can see and do what?

Over time, access permissions often drift. People change roles, leave the organisation, or gain elevated access for one-off tasks that never get rolled back. Take time to:

- **Review all user accounts:** disable or remove inactive users immediately.
- **Check roles and permissions:** do they still align with actual job duties?
- **Apply least privilege:** only grant access that's absolutely necessary.
- **Avoid using shared accounts:** especially those with administrative privileges.

2. Authentication: Strengthen your front door.

If you haven't yet enforced multi-factor authentication (MFA) for users accessing Dynamics GP—especially remote users or administrators—make that a priority. Ensure remote access is secured through VPN or approved methods, and monitor for failed login attempts.

3. Data protection: Secure at rest and in transit.

Have you checked recently whether your SQL Server databases use Transparent Data Encryption (TDE)? Are backups encrypted? Key steps include:

- **SSL/TLS encryption** for any GP database connections.
- **Regular patching** of SQL Server and Windows.
- **Storing backup copies off-network** using the 3-2-1 approach.

4. Integrations and add-ons: Know your entry points.

Dynamics GP often connects with external systems—CRM, e-commerce, payroll. Each one introduces risk. Remind your team to:

- **Audit all third-party applications** connected to Dynamics GP.
- **Use limited-permission service accounts** for integrations.
- **Monitor integration logs** for unusual behaviour.

5. Audit trails and incident response: Are you watching?

Make sure audit logging is turned on for critical activities and review these logs regularly, not just when something goes wrong. Additionally:

- **Revisit your incident response plan** and ensure your team knows the steps.
- **Simulate a breach scenario** to test preparedness and refine processes.

Compliance isn't optional

If your organisation is subject to regulations like SOX, GDPR, or local financial governance requirements, your Dynamics GP environment must reflect that. For example, if you are preparing for audit season, your Dynamics GP access logs and backup reports may be asked for. Ensuring they are configured correctly could mean the difference between a clean audit and a red flag.

Annual security reviews, evidence of access controls, and data protection measures are not just good practice, they're likely mandatory.

Security hygiene: Small steps, big impact

If you're short on time, here are some quick wins to help close security gaps:

- Change any **default passwords** still in use.
- Confirm your **latest Dynamics GP and SQL updates** are applied.
- Test your **backup restore process** – don't wait until you need it.
- Reconfirm that **audit trails** are turned on and storing data as expected.

Leveraging Intelligent Automation

Whilst Dynamics GP does not natively include AI, you can extend its security posture using Intelligent Automation (IA) tools. By integrating tools like Microsoft Power Automate, you can set up alerts for unusual login behaviour, automate user access reviews, or schedule security audits without manual effort. Similarly, Microsoft Power BI can help visualise risk trends or failed access attempts across time.

Your partner can help

If you're unsure where to begin, engage your Dynamics GP implementation partner. If we are your Dynamics GP partner, reach out for any assistance, and if we aren't your partner, feel free to ask us questions, or delve into what partnering with PA would be like.

Your partner can:

- Conduct a rapid security health check.
- Help you prioritise critical issues.
- Configure or review MFA, backups, permissions, and audit settings.
- Provide documentation for compliance reporting.
- To further ensure your security is as effective as it can be, follow industry expected risk mitigation strategies like Essential Eight.

Final thought: Security is not set-and-forget

Security needs ongoing care. Schedule regular checkpoints—monthly access reviews, quarterly security audits, and annual disaster recovery testing.

A small investment of time today could save you from major disruption tomorrow.

Your data is valuable. Your clients and stakeholders expect diligence. Make sure your Dynamics GP environment reflects that.

PA does more than just support Dynamics GP. If you are looking for a one-off security review or a full ERP modernisation, our team can help you identify gaps, prioritise improvements, and protect your financial data.

Let's talk before small gaps become big problems.

Latest Blogs

5 Tactics to Protect Privacy and Get AI Right

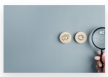
21 October 2025

Unlocking AI for finance leaders: Why ERP modernisation matters now

14 October 2025

Why Now is the Time to Move from EA to CSP with Professional Advantage

7 October 2025



Association evolution through AI transformation

30 September 2025