

Microsoft 365 Business Premium

Work from anywhere. Keep a handle on your business data.

A practical guide to the licences, setup and ongoing care behind secure everyday work.



Illustrative stock photograph: fauxels / Pexels. Not a hostme.ie customer site.

Your team needs email, files and familiar apps. You also need to know who can sign in, which devices hold work data and who can share it.

Business Premium is one way to bring those controls together. It is worth comparing with your existing setup, rather than assuming every business needs an upgrade.

The useful question is: which controls does your business need, and who will maintain them?

Inside: costs · plan comparison · practical limits · a rollout approach · a discussion checklist

Three separate decisions. Three clear cost lines.

A Microsoft licence gives access to software. Setup puts it to work. Ongoing support keeps the agreed environment maintained.

All prices exclude VAT. These are hostme.ie list prices, not a quote for your specific setup.

Microsoft licences	At cost
Business Premium, Copilot and other add-ons	Current supplier quote
Microsoft 365 specialist setup	€150 / hour
Configuration and project work	Or a scoped project quote
Managed IT — Standard	€85 / user / month
Routine support and a maintained security baseline	Minimum five managed users

What the ongoing support line means

Standard managed IT includes reactive and proactive support, monitoring and patching, licence administration, device management, backup monitoring, vendor liaison and monthly reporting. Routine work is not metered by the hour; fair use applies. Changes to the estate are separately scoped projects.

The initial term is 12 months. During that term, billing uses the greater of actual managed users, the five-user minimum or 90% of the starting count. Additions are charged in full. After the initial term, billing follows actual counts; the agreement rolls with 30 days' written notice.

Onboarding and project work

Managed onboarding starts with a **€400 assessment**, credited against the onboarding project. If you proceed to managed service and no chargeable setup is needed, it is credited against the first month instead. The setup work is quoted separately and completed before the managed fee starts.

Hourly work has a 30-minute minimum, then 15-minute increments. Work expected to exceed four hours is estimated in writing before it starts. Microsoft licences are billed separately from labour.

"Standard" in this price list is a hostme.ie support level. It is different from the Microsoft 365 Business Standard licence. You can commission a Microsoft 365 project without a managed agreement.

Service hours: Monday–Friday, 09:00–18:00, excluding Irish public holidays. Licence variant, billing frequency and subscription term are confirmed in your quote.

Compare the controls, not just the apps.

Both plans provide familiar productivity tools. Premium adds a defined set of security and management services. Existing tools and add-ons may already meet some of your needs.

Area	Business Standard	Business Premium
Everyday work	Office apps, business email and file collaboration	Those core tools, plus the services below
Sign-in controls	MFA through security defaults; other controls can be licensed separately	Entra ID P1, including Conditional Access
Devices and apps	Intune Plan 1 is not included; separate tools may be used	Intune Plan 1 for supported device and app management
Endpoint protection	Defender for Business is not included	Defender for Business for supported endpoints
Email protection	Baseline mailbox protection	Defender for Office 365 Plan 1
Sensitive data	Premium's information protection package is not included	Selected Purview features: manual labels, encryption and DLP
Paid Copilot	Eligible base plan; separate add-on required	Eligible base plan; separate add-on required

Teams inclusion depends on the purchased variant. Confirm the exact plan and all users covered by each policy. Product references: 1, 2, 4 and 6 on page 6.

When Standard may still fit

If supported security and device management are already provided through other tools, compare coverage and administration before replacing them. A move to Premium is a requirements decision, not an automatic upgrade for every business.

When Premium is worth discussing

You need central device management, more flexible sign-in rules, stronger email protection or a consistent way to handle sensitive information. Start by identifying the gap you need to close.

Useful protection. Clear boundaries.

Conditional Access is not the same as risk-based access

Premium includes Entra ID P1. Rules using sign-in risk or user risk from Entra ID Protection require P2 licensing. Do not assume those features are included in the base subscription. [2, 3]

Data protection has a defined scope

Manual sensitivity labels and foundational DLP support a useful baseline. DLP for Exchange, SharePoint and OneDrive is different from Endpoint DLP or Teams chat DLP. Advanced automatic labelling and information barriers need extra licensing; check the exact requirement. [4, 5, 10]

Copilot follows existing permissions

Copilot can use data a user is permitted to access. It does not give a Standard user unrestricted access, and Premium does not automatically repair overshared files. Review permissions and handling rules before introducing AI. Paid work-grounded Copilot is separate from Copilot Chat availability. [6, 7]

A remote wipe is not an instant guarantee

The action available depends on ownership, platform, enrolment and connectivity. Removing work data from a supported app is different from resetting a whole device. Plan the response and confirm the result when an action is used. [8]

Backup needs its own plan

Premium is not a separate Microsoft 365 backup service. Microsoft 365 Backup is billed separately. Agree recovery needs and test the chosen approach before retiring an existing backup product. [9]

Buying a licence is the start. Policies must be configured, suitable devices enrolled and responsibilities agreed. Security reduces risk; it does not guarantee that attacks, mistakes or data loss cannot happen.

A subscription does not certify GDPR compliance. Your data handling, staff practices and applicable requirements still need review.

Introduce changes without losing the thread.

A practical rollout starts with people and working habits, then introduces the controls in a planned order.

1. Understand the current environment

Identify the current licences, account owners, devices and existing security tools. Find out where staff keep work files and what they need to share. Record the gaps rather than treating every tool as redundant.

2. Agree the scope and costs

Confirm which Microsoft plan variants and add-ons are needed. Separate licence costs, setup work, recovery arrangements and ongoing care. Get a written scope before changes begin.

3. Pilot and check the controls

Use a small agreed group first. Check staff can sign in and use their work apps. Confirm device ownership, management options and the effect of file-handling policies before wider rollout.

4. Give staff clear guidance

Explain sign-in prompts, work and personal device boundaries, document labels and what to do with a suspicious message. The rules should make sense to the people expected to follow them.

5. Agree what happens afterwards

Assign responsibility for reviewing access, devices, alerts and recovery. Record joiner and leaver steps. Keep a useful record of the configuration so support is not dependent on someone's memory.

What you should be able to explain afterwards

- Which people and devices are covered.
- Which controls are active and which are outside scope.
- Who reviews issues and how staff ask for help.
- What is backed up and how recovery is checked.

Availability and supported actions vary by platform and service. Existing subscriptions, third-party systems and licence terms are checked before a change is agreed.

Bring these questions to your review.

☐ What Microsoft 365 plan do we use, and how many people need it?

☐ Which company and personal devices access work data?

☐ Who owns account access and the staff-leaver process?

☐ Where do we store sensitive files, and who can share them?

☐ Which security and backup tools are already in place?

☐ Are we planning to use Copilot, and for which tasks?

Over to you

Ask about your Microsoft 365 setup

Tell hostme.ie your team size, current plan and the problem you want to address. The next step is a scoped discussion of options and costs.

[Start a WhatsApp conversation](#)

info@hostme.ie · 089 960 2794

Galway-based, serving businesses across the west of Ireland.

Service hours: Monday–Friday, 09:00–18:00, excluding Irish public holidays.

Product references

Checked 12 October 2026. Current entitlements are confirmed when quoting. Click a reference to open Microsoft's source.

[1. Product components and plan variants](#)

[3. Risk-based policies require Entra ID P2](#)

[5. Automatic sensitivity labelling licensing](#)

[7. Copilot respects user permissions](#)

[9. Microsoft 365 Backup is separately billed](#)

[2. MFA and Conditional Access](#)

[4. Foundational labels, DLP and audit](#)

[6. Copilot licensing and eligible base plans](#)

[8. Intune wipe prerequisites and platform limits](#)

[10. Advanced Purview add-on](#)