

ANN PATEL

Northwind Traders



PREPARED BY
Harbour IT

DATE
12 Oct 2026

DATA COLLECTED
11 Oct 2026, 20:31 UTC

MICROSOFT 365 TENANT
northwindtraders.onmicrosoft.com

Everything collected about ann.patel@northwindtraders.example.

Needs attention
10
Worst: high

Sign-in
Allowed
Last sign-in 11 days ago

MFA
Protected

Admin roles
2
Global Administrator and 1 more

Licences
1 licence
£18.10 a month

Devices
2 devices

Needs attention 10 8 to review

Flag	What	Area
● High	The mailbox forwards all mail to ann.patel@homemail.example, outside the organisation.	Mailbox
● High	Inbox rule ".": Moves to RSS Feeds mail mentioning invoice, payment; Rule name '.' looks deliberately blank.	Mailbox
● High	Inbox rule "Copy to home": Forwards to ann.patel.home@homemail.example.	Mailbox
● High	Shares 1 item from OneDrive with anyone who has the link.	OneDrive
● Medium	Admin without a phishing-resistant method: register a passkey or security key. A fake sign-in page can relay codes and push approvals.	MFA and sign-in protection

Flag	What	Area
● Medium	Gave Mail Sync Pro access to Mail.Read. Check it's an app the business uses.	Apps this person allowed
● Medium	Signed in from FR, which this tenant rarely signs in from. Check the person was there.	Recent sign-ins
● Medium	Signed in 2 times with only a password in the last 7 days.	Recent sign-ins
● Low	Microsoft 365 Business Premium is assigned directly and by All Staff, so taking them out of the group won't remove it.	Licences
● Low	Microsoft 365 Business Premium: Exchange Online (Plan 2). Only used email in the last 30 days. Saves £11.50 a month.	Microsoft 365 use

Account 6

Detail	Value
Name	Ann Patel
Sign-in name	ann.patel@northwindtraders.example
Account type	Member
Sign-in	Allowed
Source	Cloud-only
Password expires	Follows the organisation's policy

Licences 1

Detail	Value
Usage location	GB

Licences 1

Licence	Assigned	Cost / month
Microsoft 365 Business Premium	Directly and by group: All Staff	£18.10

Microsoft 365 use 7

Detail	Value
Email	Used (last 10 Oct 2026)
Teams	Not in the last 30 days
OneDrive	Not in the last 30 days
SharePoint	Not in the last 30 days
Office apps	Used (last 10 Oct 2026)
Office apps used on	Web
Email in 30 days	40 sent, 300 received

Cheaper licence options 1

Flag	Licence	Option	Why	Saving / month
● Low	Microsoft 365 Business Premium	Exchange Online (Plan 2)	Only used email in the last 30 days. It also includes Intune, Entra ID P1 and Defender, which an Exchange Online plan doesn't. Check the account doesn't rely on them.	£11.50

MFA and sign-in protection 10

Detail	Value
MFA set up	Yes
Methods	Authenticator app
Phishing-resistant method	No
Strongest method	Authenticator app or token
Asked for first	Authenticator app
Can sign in without a password	No
Can reset their own password	Yes
MFA required by	Require MFA for all users
Conditional Access policies that apply	Require MFA for all users
Legacy sign-in blocked	No

Admin roles 2

Role	How assigned	Scope	Privileged
Global Administrator	Active	Whole directory	Yes
Groups Administrator	Active	Limited scope	No

Administrative units 2

Unit	Relationship	Membership	Restricted
Sales	Administers as Groups Administrator	Assigned	No
Sales	Member	Assigned	No

Teams and groups 8

Name	Type	Role	Note
Board	Team	Owner	Only owner
Clients	Team	Owner	–
Sales	Team	Owner	–
Finance	Microsoft 365 group	Owner	–
Operations	Team	Member	–
Marketing	Microsoft 365 group	Member	–
Marketing	Microsoft 365 group	Member	–
Provisioned	Microsoft 365 group	Member	–

Mailbox 8

Detail	Value
Address	ann.patel@northwindtraders.example
Type	User
Size	7.3 GB of 49.5 GB (15%)
Archive	On
Litigation hold	Off
Forwarding	ann.patel@homemail.example (outside the organisation)
Older protocols allowed	None
More	Everything about this mailbox

Inbox rules 2 2 to review

Flag	Rule	Enabled	What it does	Why it stands out
● High	.	Yes	body has invoice, payment: move to RSS Feeds; mark as read; stop processing rules	Moves to RSS Feeds mail mentioning invoice, payment; Rule name '.' looks deliberately blank
● High	Copy to home	Yes	All messages: forward to ann.patel.home@homemail.example	Forwards to ann.patel.home@homemail.example

Mailboxes this person can open or send from 3

Mailbox	Type	Access
accounts@northwindtraders.example	Shared	Full access, Send as
info@northwindtraders.example	Shared	Full access, Send as, Send on behalf
reception@northwindtraders.example	Shared	Full access, Send as

Devices 2

Device	Operating system	Compliance	Encrypted	Last check-in	Problems
Ann Patel's iPhone	iOS 18.6	Compliant	–	Today	–
LAPTOP-PATEL	Windows 11 25H2 (10.0.26200.6584)	Compliant	Yes	Yesterday	–

OneDrive 4

Detail	Value
Storage used	53.4 GB of 1.00 TB
Files	50
Files active in the last 30 days	5
Last activity	9 Oct 2026

Shared from this OneDrive 1 1 to review

Flag	File or folder	Shared with	Can edit	Link expires
● High	holiday.jpg	Anyone with the link	No	1 Jan 2099

Apps this person allowed 1 1 to review

Flag	App	Publisher	Permissions	From
● Medium	Mail Sync Pro	Unknown Ltd (unverified)	Mail.Read, offline_access	Third party

Recent sign-ins 8

Detail	Value
Successful	34 (32 with MFA, 2 with only a password)
Failed	3 (3 wrong password, from 3 addresses)
MFA and other prompts	2
Last failure	8 Oct 2026 (3 days ago): Wrong user name or password
Countries	GB, FR (unusual for this tenant), RU, BR
Apps	Microsoft Teams, Office 365 Exchange Online, Office 365 SharePoint Online, Azure Portal, Unknown app
Devices	Windows10
Addresses that failed	203.0.113.42, 198.51.100.9, 203.0.113.66

Where this account signed in 4 1 to review

Flag	Country	Successful	Failed	Cities	IP addresses	Last success (UTC)
	GB	33	1	London	192.0.2.10, 203.0.113.42	10 Oct 2026, 16:15
● Medium	FR	1	0	Paris	198.51.100.40	8 Oct 2026, 21:40
	BR	0	1	Sao Paulo	203.0.113.66	–
	RU	0	1	–	198.51.100.9	–

Why sign-ins failed 1

Error code	What it means	Sign-ins
50126	Wrong user name or password	3

Sign-in history 3

Detail	Value
History from	13 Jun 2026
Last sign-in	10 Oct 2026 (yesterday)
Countries	BR, FR, GB, IE, RU, US

Sign-ins by month 5

Flag	Month	Days	Successful	Failed	With MFA	Password only	Countries
● Low	Oct 2026	7	39	3	35	4	BR, FR, GB, IE, RU
● Low	Sep 2026	20	41	0	30	11	GB, IE
● Low	Aug 2026	19	40	1	31	9	FR, GB, IE
● Low	Jul 2026	23	51	2	27	24	FR, GB, US
● Low	Jun 2026	12	28	0	19	9	FR, GB, IE, US

Sign-ins and admin changes 3

Detail	Value
Last interactive sign-in	30 Sep 2026 (11 days ago)
Last background sign-in	None recorded
Last successful sign-in	None recorded

Legacy sign-ins in the last 30 days 1

Flag	Client	Succeeded	Failed	Last attempt	Countries
● Low	IMAP4	0	1	7 Oct 2026 (4 days ago)	RU

Admin changes in the last 120 days 3 1 to review

Flag	When (UTC)	Change	By	Target	Detail
● Medium	8 Oct 2026, 20:31	Add eligible member to role in PIM completed (permanent)	admin@northwindtraders.example	ann.patel@northwindtraders.example	Exchange Administrator
	8 Oct 2026, 08:31	Reset user password	admin@northwindtraders.example	ann.patel@northwindtraders.example	–
	7 Oct 2026, 08:31	Admin registered security info	admin@northwindtraders.example	ann.patel@northwindtraders.example	–

Timeline 13 8 to review

Flag	When	Area	What happened
● Medium	8 Oct 2026, 21:40 UTC	Sign-in	Signed in from FR, unusual for this tenant (198.51.100.40)
● Medium	8 Oct 2026, 20:31 UTC	Admin change	Add eligible member to role in PIM completed (permanent): Exchange Administrator (by admin@northwindtraders.example)
	8 Oct 2026, 16:07 UTC	Sign-in	Last of 3 failed sign-ins: Wrong user name or password
	8 Oct 2026, 08:31 UTC	Admin change	Reset user password (by admin@northwindtraders.example)
	7 Oct 2026, 08:31 UTC	Admin change	Admin registered security info (by admin@northwindtraders.example)
	7 Oct 2026, 03:00 UTC	Sign-in	Legacy sign-in with IMAP4: 0 succeeded, 1 failed
● High	On or before 6 Sep 2026	Mailbox	Inbox rule "." first seen: Moves to RSS Feeds mail mentioning invoice, payment; Rule name '.' looks deliberately blank
● High	On or before 6 Sep 2026	Mailbox	Inbox rule "Copy to home" first seen: Forwards to ann.patel.home@homemail.example

Flag	When	Area	What happened
● High	On or before 6 Sep 2026	Mailbox	Forwarding to ann.patel@homemail.example first seen (outside the organisation)
● Medium	On or before 6 Sep 2026	Apps	Allowed Mail Sync Pro (Mail.Read, offline_access)
	On or before 6 Sep 2026	MFA	Authenticator app first seen as an MFA method
● Medium	On or before 6 Sep 2026	Admin roles	Global Administrator role first seen
● Medium	On or before 6 Sep 2026	Admin roles	Groups Administrator role first seen

Open findings 5 4 to review

Flag	Check	Detail	First seen
● High	No inbox rules hide mail	": Moves to RSS Feeds mail mentioning invoice, payment; Rule name '!' looks deliberately blank	6 Sep 2026
● High	No mail is forwarded outside the organisation	Mailbox forwarding to ann.patel@homemail.example (keeps a copy)	6 Sep 2026
● High	No mail is forwarded outside the organisation	Inbox rule "Copy to home" forwards to ann.patel.home@homemail.example	6 Sep 2026
● Medium	Admins use phishing-resistant sign-in methods	Global Administrator; signs in with Authenticator app	6 Sep 2026
● Low	No account reports to a blocked manager	Reports to Robert Hughes, whose sign-in is blocked	6 Sep 2026

History 0

No changes recorded yet.

Prepared by Harbour IT (help@harbourit.example · 0161 496 0000). Read from Microsoft 365 with read-only access; nothing was changed. Data collected 11 Oct 2026, 20:31 UTC.