

Example, not a real client. Example Lettings Ltd, every name and every .example address in this document are made up. This shows the format of a Clarwyn IT Security Review and Remediation report.

Security Review and Remediation: Example Lettings Ltd

Prepared for: Example User 1, Director, Example Lettings Ltd
Prepared by: Jamie Castle, Clarwyn IT
Review date: 2 November 2026. **Report version:** 2 (after remediation, 6 November 2026)
Scope: the Microsoft 365 account for example-lettings.example, 8 users, checked against Clarwyn IT's defined checklist.

How to read this report

- Red:** a real risk that should be fixed now. Every red item is fixed once you approve it in writing.
- Amber:** worth improving. These are recommendations; any work on them is quoted separately in writing before it starts.
- Green:** in good shape.

1. Summary

Example Lettings' Microsoft 365 was working well day to day, but some important protections were missing. Two people could sign in with a password alone, three everyday accounts had full admin rights, two former staff accounts were still active, and one mailbox was quietly forwarding all mail to an outside address. All eight red items were approved in writing on 4 November and fixed by 6 November.

	Red	Amber	Green
Found on 2 November	8	3	2
After remediation, 6 November	0	4	9

2. Findings

#	Area	Check	What we found	Rating	Recommendation	Status
1	Multi-factor sign-in	Required for every user	6 of 8 users registered; nothing required the other 2 to use it	Red	Require multi-factor sign-in for everyone	Fixed 5 Nov. Now green
2	Multi-factor sign-in	Older sign-in methods that skip it are blocked	Allowed	Red	Block them	Fixed 5 Nov. Now green
3	Admin roles	Number of full (Global) administrators	3, all on everyday mailboxes	Red	Use a separate admin account; remove admin rights from everyday accounts	Fixed 5 Nov. Now green
4	Admin roles	Admin accounts use multi-factor sign-in	1 of 3 did	Red	Covered by items 1 and 3	Fixed 5 Nov. Now green

#	Area	Check	What we found	Rating	Recommendation	Status
5	Dormant accounts	Accounts of people who have left	2 former staff accounts could still sign in	Red	Block sign-in; keep the mail as agreed	Fixed 5 Nov. Now green
6	Dormant accounts	Accounts with no sign-in for 90 days or more	1 (a temporary account from the summer)	Amber	Remove if no longer needed	Recommendation
7	Email protection	Anti-phishing settings	Microsoft's default settings only	Amber	Consider stronger impersonation protection, which needs a different licence	Recommendation
8	Email protection	Spoofing: SPF record	Present and correct	Green	None	n/a
9	Email protection	Spoofing: DKIM and DMARC	DKIM off; no DMARC record	Red	Turn on DKIM; publish DMARC in monitoring mode	Fixed 5 Nov. Now amber: move DMARC to quarantine once reports are clean
10	Email protection	Automatic forwarding to outside addresses	Allowed, and 1 mailbox rule forwarded all mail to an outside address	Red	Remove the rule (after checking with the user) and block automatic outside forwarding	Fixed 5 Nov. Now green
11	OneDrive and SharePoint	"Anyone" links (open to anyone with the link)	14 such links to a folder of tenancy documents, with no expiry	Red	Remove the links to sensitive files; reshare with named people	Fixed 6 Nov. Now green
12	OneDrive and SharePoint	Default sharing link type	"Anyone with the link"	Amber	Change the default to "People in your organisation"	Recommendation
13	OneDrive and SharePoint	Sharing with guests	Allowed with named guests only	Green	None	n/a

3. Approval for red items

The red items above were sent to Example User 1 for approval on 2 November. Approved in writing ("approved") by Example User 1 on 4 November, for items 1, 2, 3, 4, 5, 9, 10 and 11. Your team received a short guide before multi-factor sign-in was required.

4. Amber items: optional further work

#	Item	Why it matters	Next step
6	Remove the unused temporary account	Unused accounts are an easy way in if their password leaks	Quoted separately, or included in Clarwyn Care
7	Stronger anti-phishing (impersonation protection)	Helps catch emails pretending to be you, landlords or suppliers	Needs a licence that includes it; we can advise on the cost

#	Item	Why it matters	Next step
9	Move DMARC from monitoring to quarantine	Stops others sending fake email that looks like yours	Quoted separately, or included in Clarwyn Care
12	Default sharing link type	Reduces the chance of files being shared more widely than intended	Quoted separately, or included in Clarwyn Care

5. Changes made

Date	Change	Item
5 Nov 2026	Multi-factor sign-in required for all users; older sign-in methods blocked	1, 2, 4
5 Nov 2026	Separate admin account created, plus 1 emergency (break-glass) admin account kept for use only if normal admin sign-in fails; admin rights removed from 3 everyday accounts	3
5 Nov 2026	Sign-in blocked for 2 former staff; their mail kept in shared mailboxes, as you asked	5
5 Nov 2026	DKIM turned on; DMARC published in monitoring mode	9
5 Nov 2026	Outside forwarding rule removed (confirmed with the user); automatic outside forwarding blocked	10
6 Nov 2026	14 "Anyone" links to tenancy documents removed; files reshared with named people	11

6. Limits of this review

This review covers the Microsoft 365 settings listed above, on the dates shown. It doesn't cover devices, other software, networks, physical security or staff behaviour. It isn't a penetration test or a certification, such as Cyber Essentials. Settings can change after the review date.

One-page summary (for insurers and customers)

Example Lettings Ltd: Microsoft 365 security summary

Date: 6 November 2026. **Reviewed by:** Jamie Castle, Clarwyn IT. **Users covered:** 8.

Example Lettings Ltd had its Microsoft 365 reviewed against a defined checklist covering multi-factor sign-in, admin roles, dormant accounts, email protection (anti-phishing, spoofing and forwarding) and OneDrive and SharePoint sharing. All items rated red were fixed by 6 November 2026.

Control	Position on 6 November 2026
Multi-factor sign-in required for all users	Yes
Multi-factor sign-in required for all admin accounts	Yes
Older sign-in methods that skip multi-factor sign-in blocked	Yes
Admin accounts separate from everyday accounts	Yes
Number of full administrators	2 (including 1 emergency account)
Former staff accounts blocked	Yes
Anti-phishing protection	Microsoft's standard protection on
SPF, DKIM and DMARC published for example-lettings.example	Yes (DMARC in monitoring mode)
Automatic forwarding of email to outside addresses	Blocked
"Anyone" sharing links to sensitive files	Removed

Outstanding recommendations: move DMARC to quarantine; stronger impersonation protection; change the default sharing link type.

This summary describes Microsoft 365 settings on the date shown. It is not a certification.

Jamie Castle trading as Clarwyn IT, sole trader. hello@clarwyn.co.uk. Example, not a real client.