

Buildings Security Assessment Form and Action Plan

Building Assessed: Marksbury Road

Assessed By: Amelia Bell

Date of risk assessment: 24/08/2026

Date of previous risk assessment: 30/06/2026

1. Is access to the outside of the building controlled i.e. covered by CCTV?		
No	Risk Level: High	Action Plan: Entrances and car park covered by CCTV, however only accessible by Marksbury Operations Manager. Intercom camera on backdoor currently broken.
2. Does the outside of the building have security lighting, floodlighting or street lighting?		
Yes	Risk Level: Medium	Action Plan: Lighting at entrance and in car park
3. Are there warnings on windows, visible alarms etc that warn potential intruders that there are physical security measures in place?		
Yes	Risk Level: Low	Action Plan: CCTV signage, and also visible alarm box on building.
4. Are accessible windows suitably protected with locks?		
Yes	Risk Level: Low	Action Plan:
5. Do the downstairs windows have security bars?		
No	Risk Level: Medium	Action Plan:
6. Are the windows closed and checked every evening?		
Yes	Risk Level: Medium	Action Plan: The cleaner closes the windows after the weekday daytime service and host will do the remaining as part of closing down procedure.

7. Are blinds closed and checked every evening?		
N/A	Risk Level: Low	Action Plan: Building always in use
8. Are skylights suitably protected by bars and locks?		
Yes	Risk Level: Low	Action Plan: Skylight locked
9. Are external doors suitably protected e.g. by 5 lever locks?		
Yes	Risk Level: Medium	Action Plan: All external doors are suitably protected.
10. Is there a burglar alarm with intruder monitors covering all areas especially those containing IT equipment or records?		
Yes	Risk Level: Medium	Action Plan: Yes, but not in use as building in constant use
11. Is the alarm system connected to a police station or call response centre?		
Yes	Risk Level: Medium	Action Plan: The intruder alarm system is only activated during Business Continuity Plan (BCP) situations when the building is unoccupied. During normal operations, the alarm is not set.
12. Are you able to ensure all keys stored on site are not obvious and any instructions regarding key instructions or keypad codes are stored securely?		
Yes	Risk Level: Medium	Action Plan:
13. Are keypad codes changed regularly?		
Yes	Risk Level: Low	Action Plan: Keypads are only used by Brisdoc and updated every 6 months by the facilities team, the practice use swipe cards to access their equipment.
14. Are alarm codes changed regularly?		
No	Risk Level:	Action Plan: Intruder alarm not in use during normal operations as the building is occupied; low risk.

	Medium	Access via the rear door is controlled by a keycode, which presents a greater security risk if the code becomes known to unauthorised individuals.
15. Are staff aware of the procedure for challenging unidentified visitors in controlled areas?		
Yes	Risk Level: High	Action Plan: Staff are aware of the requirement to challenge individuals who are not recognised and follow established procedures, including seeking assistance where required. However, due to the current failure of the magnetic lock/intercom system and the need for manual locking and unlocking of the door, there is an increased risk of unauthorised access as controls are reliant on human intervention and therefore susceptible to error.
16. Do staff ensure that the Drug Cupboard or the access to the Drug Cupboard is logged and managed appropriately?		
Yes	Risk Level: Medium	Action Plan: Drug cupboard is locked at all times, key for the cupboard is locked in a key safe in the store cupboard. Process for management of drugs in place.
17. Do staff ensure that paperwork is not left unattended in the Consultation Area or other sensitive areas?		
Yes	Risk Level: Medium	Action Plan: Staff are required to do GDPR training as part of their Mandatory training annually.
18. Are screensavers in use on computers that are used to display information about patients?		
Yes	Risk Level: Medium	Action Plan: Staff hold responsibility to lock their screen if they are away from their desk.
19. Are identity passes/cards worn by all staff at all times?		
Yes	Risk Level: Low	Action Plan: Staff are required to wear their name badges at all times
20. Are identity passes/cards worn by all visitors at all times?		

Yes	Risk Level: Low	Action Plan: Visitors are given a visitors pass when signing in to the visitor's book.
21. Are visitors escorted at all times in secure areas?		
Yes	Risk Level: Low	Action Plan: Visitors are for planned reasons and have an escorting employee attached to their visit.
22. Is a log of visitors maintained?		
Yes	Risk Level: Low	Action Plan: Staff are required to log visitors in the Visitors book so we have a record of them being there if we were to have any problems
23. Is IT equipment situated where it cannot be viewed by visitors or the public from outside the premises?		
Yes	Risk Level: Low	Action Plan:
24. Are deliveries to and collections from the site, supervised?		
Yes	Risk Level: Low	Action Plan:
25. If a back door or loading bay is used to receive deliveries – is this secured when not in use?		
N/A	Risk Level: Low	Action Plan: No loading bay
26. Is new equipment stored securely prior to installation?		
Yes	Risk Level: Low	Action Plan:
27. Is the movement of IT equipment out of the site subject to authorisation and control? i.e. use of laptops and portable equipment off site.		
Yes	Risk Level: Low	Action Plan: All IT equipment is permanent and no laptops are in use.
28. Are lock down devices used to secure IT equipment?		

No	Risk Level: Medium	Action Plan: PCs are password protected. Clinical system require personal login.
29. Are laptops and other portable equipment stored securely overnight?		
Yes	Risk Level: Low	Action Plan: Mobile phones are kept in store cupboard accessed via keypad code entry or in rooms locked when not in use.
30. Are back-up Tapes stored securely, for example in the site safe?		
N/A	Risk Level: High/Low/Medium	Action Plan:
31. Is IT equipment asset marked?		
Yes	Risk Level: Low	Action Plan:
32. Do assets have visible ID markings?		
Yes	Risk Level: Low	Action Plan:
33. Is electronic equipment stored away from the risk of burst water pipes?		
Yes	Risk Level: Low	Action Plan:
34. Is electronic equipment stored away from the risk of splashing from taps or sinks and the risk of water running from windows or condensation?		
Yes	Risk Level: Low	Action Plan:

Any there any other observations from the review?

Risk Assessment needs updating when intercom system repaired

Date of Next Review: 10/03/2027

Review Carried Out By: Amelia Bell

Action Plan Follow-up Date: None, all actions already in place