

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| < Insert name of pharmacy>  **Physical security risk assessment** | | | | <Insert pharmacy logo> |
| Doc prepared by: | Doc approved by: | Date next review due: |  |  |
| Date prepared: | Date approved: | Date review takes place: |  |  |

|  |
| --- |
| ***About the use of this document and related resources****: This* [*data security*](http://psnc.org.uk/ds) *document assists the pharmacy’s aligment with the*[*Data Security and Protection Toolkit (DSPTK)*](http://psnc.org.uk/dsptk)*. Related pharmacy policies are at PSNC’s* [*data security templates webpage*](http://psnc.org.uk/dstemplates)*.* |

*The level of risk is normally established by considering the impact of a potential data loss occurring and the likelihood of a loss taking place. It is for a contractor to assess the risk based on local circumstances and take a decision on which physical security measures are appropriate.*

|  |  |  |
| --- | --- | --- |
| **1. Is access to the outside of the building controlled i.e covered by CCTV?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **2. Does the outside of the building have security lighting, floodlighting or street lighting?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **3. Are there warnings on windows, visible alarms etc that warn potential intruders that there are physical security measures in place?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **4. Are accessible windows suitably protected with locks?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **5. Do the downstairs windows have security bars?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **6. Are the windows closed and checked every evening?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **7. Are blinds closed and checked every evening?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **8. Are skylights suitably protected by bars and locks?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **9. Are external doors suitably protected e.g. by 5 lever locks?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **10. Is there a burglar alarm with intruder monitors covering all areas especially those containing IT equipment or records?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **11. Is the alarm system connected to a police station or call response centre?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **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 / No | Risk Level:  High/Low/Medium | Action Plan: |
| **13. Are keypad codes changed regularly?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **14. Are alarm codes changed regularly?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **15. Are staff aware of the procedure for challenging unidentified visitors in controlled areas?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **16. Do staff ensure that the Dispensary or the access route to the Dispensary is never left unoccupied whilst the pharmacy is open?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **17. Do staff ensure that paperwork (e.g. NMS forms) is not left unattended in the Consultation Area?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **18. Are screensavers in use on computers that are used to display information about patients?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **19. Are identity passes/cards worn by all staff at all times?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **20. Are identity passes/cards worn by all visitors at all times?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **21. Are visitors escorted at all times in secure areas?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **22. Is a log of visitors maintained?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **23. Is IT equipment situated where it cannot be viewed by visitors or the public from outside the premises?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **24. Are deliveries to and collections from the pharmacy, supervised?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **25. If a back door or loading bay is used to receive deliveries – is this secured when not in use?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **26. Is new equipment stored securely prior to installation?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **27. Is the movement of IT equipment out of the pharmacy subject to authorisation and control? i.e. use of laptops and portable equipment off site.** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **28. Are lock down devices used to secure IT equipment?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **29. Are laptops and other portable equipment stored securely overnight?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **30. Are back-up Tapes stored securely, for example in the pharmacy safe?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **31. Is IT equipment asset marked?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **32. Do assets have visible ID markings?** | | |
| Yes / No | Risk Level:  High/Low/Medium | Action Plan: |
| **33. Is electronic equipment stored away from the risk of burst water pipes?** | | |
| Yes / No | Risk Level:  High/Low/Medium | 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 / No | Risk Level:  High/Low/Medium | Action Plan: |

|  |
| --- |
| **Any there any other observations from the review?** |

|  |
| --- |
| *This data security policy assist the pharmacy’s aligment with the Data Security and Protection Toolkit (DSPTK). Related pharmacy policies and more can be found at:*   * [*psnc.org.uk/ds*](http://psnc.org.uk/ds)*;* * [*psnc.org.uk/dsptk*](http://psnc.org.uk/dsptk)*; and* * [*psnc.org.uk/dstemplates*](https://psnc.org.uk/dstemplates)*.*   *Pharmacy contractors with queries about the original template or questions about DSPTK may contact* [*it@psnc.org.uk*](mailto:it@psnc.org.uk)*.* |