Dr MB Ghafoor & Dr SA Abbasi

Risk Assessment Form

Dr MB Ghafoor & Dr SA Abbasi	01.01.2018/19	Dr MB Ghafoor

Assessing the level of risk

	LIKELIHOOD				
IMPACT	**Probable**	**Possible**	**Unlikely**	**Rare**	**Negligible**
Catastrophic	**HIGH**	**HIGH**	**HIGH**	**MEDIUM**	**LOW**
Major	**HIGH**	**HIGH**	**MEDIUM**	**MEDIUM**	**LOW**
Moderate	**HIGH**	**MEDIUM**	**MEDIUM**	**LOW**	**VERY LOW**
Minor	**MEDIUM**	**MEDIUM**	**LOW**	**LOW**	**VERY LOW**
Insignificant	**LOW**	**LOW**	**VERY LOW**	**VERY LOW**	**VERY LOW**

Section 1 - Physical Security of Premises and Equipment

1 Is access to the outside of the building(s) restricted, i.e. by perimeter fencing?

Yes	**No**
Yes	

If no, the risk is classed as

Low	**Medium**	**High**

2 Is access to the outside of the building controlled i.e. covered by CCTV?

Yes	**No**
Yes	

If no, the risk is classed as

Low	**Medium**	**High**

3 Does the outside of the building have security lighting, floodlighting or street lighting?

Yes	**No**
yes	

If no, the risk is classed as

Low	**Medium**	**High**

4 Are there warnings on windows, visible alarms etc that warn potential intruders that there are physical security measures in place?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

5 Are accessible windows suitably protected with locks?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

6 Do the downstairs windows have security bars?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

7 Are the windows closed and checked every evening?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

8 Are blinds closed and checked every evening?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

9 Are skylights suitably protected by bars and locks?

Yes	No
n/a	

If no, the risk is classed as

Low	Medium	High

10 Are external doors suitably protected e.g. by 5 lever locks?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

11 Are all external doors solid e.g. not glass?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

12 Is there a burglar alarm with intruder monitors covering all areas especially those containing IT equipment or records?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

13 Is the alarm system connected to a police station or call response centre?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

14 Are there appropriate locks or keypad access on all doors containing IT equipment and records?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

15 Are you able to seal off separate areas of the building e.g. in reception are there shutters and lockable doors?

Yes	No
yes	

If no, the risk is classed as

Low	Medium	High

16 Do all consulting rooms have separate door locks?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

17 When the building is not fully occupied e.g. out of hours clinic, are unused areas, such as administrative offices secured?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

18 Are you able to ensure all keys stored on site are not obvious and any instructions regarding key locations or keypad codes are stored securely?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

19 Are staff aware of the procedure for challenging unidentified visitors in controlled areas?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

20 Are keypad codes are changed regularly?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

21 Are alarm codes are changed regularly?

Yes	No
N/A	

If no, the risk is classed as

Low	Medium	High

22 Are identity passes/cards worn by all staff at all times?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

23 Are identity passes/cards worn by all visitors at all times?

Yes	No
	No

If no, the risk is classed as

Low	Medium	High
Yes		

24 Are visitors escorted at all times in secure areas?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

25 Is a log of visitors maintained?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

26 Is IT equipment situated where it cannot be viewed by visitors or the public from outside the premisis?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

27 Are deliveries to and collections from the practice, supervised?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

28 Is new equipment stored securely prior to installation?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

29 Is the movement of IT equipment out of the Practice subject to authorisation and control?

Yes	No
N/A	

If no, the risk is classed as

Low	Medium	High

30 Are lock down devices used to secure IT equipment?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

31 Are laptops and other portable equipment stored securely overnight?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

32 Is IT equipment asset marked?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

33 Do assets have visible ID markings?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

34 Are assets UV marked with the practice post code?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

35 Is all IT equipment recorded with serial numbers on an asset register?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

Section 2 - Environmental Security

1 Is the server protected by UPS (uninterrupted power supply)?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

2 Is the battery checked on a regular basis i.e. weekly / monthly?

Yes	No
N/A	

If no, the risk is classed as

Low	Medium	High

3 Are the wiring plugs PAT checked annually?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

4 Is there a 'Fireproof' safe available for back-up tapes and other sensitive media or a documented 'off site' back-up system in place?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

5 Is the server stored in a lockable room or lockable cupboard and at an appropriate temperature?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

6 Is the server secured in a cage or locked down with a cable?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

7 Is the server sited above ground floor?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

8 Are server room windows protected?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

9 Are there Co2 fire extinguishers available and are they serviced by contract?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

10 Are you able to ensure that paper is not stacked on top or near PC's?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

11 Are you able to ensure that PC ventilators are kept clear?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

12 Is electronic equipment stored away from the risk of burst water pipes?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

13 Is electronic equipment stored away from the risk of splashing from taps or sinks?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

14 Is electronic equipment stored away from risk of water running from windows or condensation?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

Section 3 - Unauthorised Access Risk

1 Is data entry restricted to trained and authorised personnel (including locums)?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

2 Do all users have a unique ID and Password?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

3 Are all staff aware that passwords should not be divulged for any reason and that smartcards should be used ONLY by the registered user?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

4 Are passwords changed at regular intervals?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

5 Are staff advised to log out at all times if leaving the workstation?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

6 Are there automatic (3 minute) screen savers in place?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

7 Do you have a 'who', 'what', 'when' full audit trail in place?

Yes	No
N/A	

If no, the risk is classed as

Low	Medium	High

8 Is the anti-virus software updated daily? **(PC's on the tPCT network are updated daily)**

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

9 Do the staff know how to check that the update has taken place?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

10 Do staff use the anti-virus software installed for checking external sources?

Yes	No
N/A	

If no, the risk is classed as

Low	Medium	High

11 Are there maintenance contracts with guaranteed response times for Non tPCT equipment?

Yes	No
N/A	

If no, the risk is classed as

Low	Medium	High

12 Are back-ups taken daily and stored adequately?

Yes	No
N/A	

If no, the risk is classed as

Low	Medium	High

13 Is there a procedure for checking that back-ups work ?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

14

Is there a senior member of staff who is responsible for Health and Safety issues?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

15 Are all workstations connected to a LAN (Local Area Network)?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

16

Are all external communications connected to the organisations LAN, authorised?

Yes	No
Yes	

If no, the risk is classed as

Low	Medium	High

17 Does the disaster recovery plan/BCP allow for full running 'off site' in the event that the building is unusable (i.e. hard and software and data)?

Yes	No

Yes	

If no, the risk is classed as

Low	Medium	High

- **Level 2**

Having identified any areas of risk, the Practice should weigh the risks against the likelihood of

Where the risk of a breach in security is likely, the Practice should develop an action plan and

Where the perceived risk is low, the Practice may decide that action is unnecessary at this time;

The Practice should implement its action plan by beginning to make the improvements

- **Level 3**

The Practice has taken all reasonable steps to ensure its property is physically secured. This will

Physical security should be subject to regular risk assessment and updated guidance/