Priomh Security Inc. Office Security Checklist

This document lists a series of simple steps you can take to help ensure the security of your office spaces & valuable information assets. It is designed to provide you with a basic model which can be tailored to fit your specific business needs and should be used in conjunction with a robust security risk management plan.

Priomh Security provides specialist security advice to businesses of all sizes and we are happy to assist you in with the development and deployment of your security plans. Based in the Denver Metro area, we have experience dealing will clients of all sizes from small start-ups to multinational corporations.

Contact us today for a no-obligation discussion on how we can assist you.

(720) 410-1449
farah@priomhsecurity.com

Physical Security Checklist

1. Examine the doors & windows – look for signs of damage, wear and tear or previous attempts to force an entry. Repair any damage found.

2. Check locks – these should be fitted to all doors and windows and suitable for the area. External doors should be fitted with locks that meet a recognized security standard.

3. Inspect locks – look for signs of damage, ensure the locking mechanisms work properly, look for signs of attempted entry. Make sure the keys work and that spare keys are stored securely.

4. Make an inventory of all your important equipment, including computers & monitors, recording serial numbers and dates of purchase.

5. Classify offices / interior spaces – identify where important or valuable documents are stored and ensure these rooms are locked when not in use.

6. Put servers and other important equipment in dedicated rooms, ideally with locked internal doors and no windows or external walls.

7. Ensure all computer monitors, TV screens or other display equipment are turned off when not in use. Not only will this reduce electricity charges and carbon emissions but it reduces the tell-tale glow at night.

8. Put permanent labels on all your valuable equipment – ideally use a visible label and ultraviolet marking.

9. In shared areas, open plan offices and publicly accessible areas use cable locking systems to secure valuable equipment, such as laptops, to desks.

10. Enforce a "clear desk" policy where all paper and documents are locked away at the end of the working day. In addition to improving security, this helps reduce the effects of fires.

11. If you have multiple staff issue identity badges to your staff and encourage them to challenge unescorted visitors.

12. Keep a visitor book recoding times in and out for all visitors, consider issuing visitor badges and have a separate book for recording access to sensitive areas.

13. Escort all visitors – make sure they are not left unattended as this not only reflects badly on your business but places your commercially sensitive information at risk.

14. Consider CCTV in critical areas, such as server rooms, or areas where staff are vulnerable, such as parking spaces. This requires specialist advice so always get a full CCTV survey before you purchase any equipment.