Top 10 Security Tips for **Closed Business Premises**

If you have been instructed by the government to close your business in line with the Covid-19 guidance or you have chosen to close, it is a good time for you to review your security to reduce the chances of your premises being targeted by opportunist thieves, or your business being subjected to cyber attacks.

Secured by Design, the Police Digital Security Centre and the National Counter Terrorism Security Office have put together the Top 10 Security Tips for Closed Business Premises, the Top 10 Cyber Security Tips for Working at Home and the latest Counter Terrorism advice following the launch of a new app. This leaflet will help you carry out a simple security risk assessment of your business premises and cyber security and identify any obvious vulnerabilities.

1 **Property maintenance** You should check your premises regularly, at least once a week, to see if there are any obvious signs of an attempted break-in or damage. It is important that premises continue to be well-maintained during this extended period of closure to prevent the spiral of decline. This includes removing litter and graffiti as soon as possible and making sure that landscaping is cut back to assist with surveillance from passers-by and your CCTV system. Flammable and combustible materials and substances should be stored in a secure, lockable container, cage or room. Bins should be securely stored away from the building to prevent arson.

2 **Monitored intruder alarm system** A monitored intruder alarm system is a deterrent to burglary as it increases the likelihood of being caught. Make sure it is regularly maintained, in good working order and is remotely monitored for a police response by a National Police Chiefs' Council compliant Alarm Receiving Centre (ARC). Ensure that staff are familiar with opening and closing procedures to prevent false alarm activations. Update your key holder list and share it with third parties, where necessary, e.g. your intruder alarm company.

3 **Security fogging system** A security fogging system is triggered by an alarm sensor and will instantly fill the area you are trying to protect with a dense, harmless fog that reduces visibility, making it virtually impossible for an intruder to access the items they want to steal. If you already have such a system, check with your supplier that it is still in good working order.

4 **CCTV** If you have CCTV, make sure it is regularly maintained, in good working order with sufficient storage capacity and as a minimum, is providing coverage of the most vulnerable areas, including doors and windows where access is likely to be gained. The recording equipment should be kept in a secure cabinet inside a lockable room within the building. All CCTV should comply with the Information Commissioner's Office guidance, see www.ico.org.uk

5 **Doors and windows** Doors and easily accessible windows should be in good working order, free from rot or damage and have good quality locks that have a Kitemark showing that they meet the relevant British Standard. There are various types of doors and windows, e.g. U-PVC, aluminium, timber, etc. and these may have multi-point or single-point locking mechanisms. All external doors should have a minimum of two locking points with locks that meet the British Standard. All doors and windows that are not part of a designated fire escape route, should be closed and locked.

6 **Glazing** All easily accessible glazing should be laminated to resist forced entry. Double glazed units only require either the inner or outer pane to be laminated. Alternatively, security film can be applied to the internal glazed panel, ensuring it is fixed under the beading, where possible.

7 **Roller shutters and grilles** Roller shutters and grilles can provide additional protection to external doors and windows in vulnerable areas around your business premises. They are particularly useful for protecting recessed doors that create hiding places because they are set back from the building line. If you have roller shutters or grilles fitted, use them.

8 **Lighting** The need for external lighting will be determined by local circumstances and the quality of street lighting in the area, e.g. inner city, rural, adopted, non-adopted areas, etc. Internal lighting should be operated by detection devices which will automatically switch lights on where movement is detected. Check that all lights are in good working order.

9 **Safe storage of valuables, assets and stock** Valuables, assets and stock should be either removed from the premises or stored in a secure, lockable container, cage or room and the keys stored in a secure key cabinet or removed entirely. It is advisable to check the continued performance of essential equipment and services, such as fridge freezers, electrical and water supplies, including central heating pipework.

10 **Gaming and vending machines** Gaming and vending machines should be emptied of all stock and cash with visible external facing signage displayed to advertise this fact and deter a potential intruder.

Secured by Design is a national police initiative which for many years has worked alongside the UK Police Service to develop minimum police preferred standards for security. For further advice about any of the 10 security tips listed above or for product procurement of police preferred products, visit: www.securedbydesign.com

Secured by Design
SBD
Official Police Security Initiative

PDSC
POLICE DIGITAL SECURITY CENTRE

NaCTSO
National Counter Terrorism Security Office

Top 10 Cyber Security Tips for **Working at Home**

1 **Strong password policy** Use a strong password for all devices and social media accounts. Change default passwords on all your devices when initially installed (especially your Wi-Fi router at home or any Internet of Things devices you may have) and consider using password managers to store and protect your passwords.

2 **2FA** Turn on the two-factor authentication setting on all your accounts and devices.

3 **VPN** Use a Virtual Private Network (VPN) to protect and encrypt the data you send or receive. It will also scan devices for malicious software.

4 **Software update** Set all your devices and apps to download and install updates automatically to ensure that any crucial fixes are not missed and the risk of your devices being infected with malware is reduced.

5 **Back up** To safeguard your most important personal data and information, back them up to an external hard drive or cloud-based storage system.

6 **Phishing emails** Cyber criminals are targeting people and businesses with fake emails about the coronavirus. Phishing emails may appear genuine but are embedded with a virus that could compromise your device, as well as manipulate you into sharing personal or financial information.

7 **Install anti-virus** Install and activate anti-virus software on all your devices, preferably set it to update automatically. This will help you to run a complete scan of your system and check for any malware infections.

8 **Safe online browsing** Only visit trusted websites especially when online shopping. Keep an eye out for websites that have a padlock sign in the address bar, as this shows that the connection and your personal information (e.g. credit card information) is encrypted and secure.

9 **Social media** It is important to review the privacy, password and security settings for all your social media accounts to ensure they are as secure as possible.

10 **Communication** Maintain contact with your team, as it is easy to feel isolated or lose focus when working at home.

More information on working from home is available from the National Cyber Security Centre: https://www.ncsc.gov.uk/guidance/home-working

For more information from the Police Digital Security Centre, visit: www.policedsc.com

New Counter Terrorism ACT App Launched

Despite the current threat from Covid-19, it is still important to remain alert and vigilant to terrorist activity.

Live-time information from Counter Terrorism Policing, plus all the very latest protective security advice, is now available at your fingertips 24/7 – wherever you are.

If you have a phone then you can keep updated where and when it matters most – all through the new easy-to-navigate Action Counters Terrorism (ACT) app.

More than a thousand specialists from across the UK have been helping officers trial this new product, including leading organisations from the security, sporting and retail sectors.

COUNTER TERRORISM POLICING
ACT ACTION COUNTERS TERRORISM
IN THE RARE EVENT OF
a firearms or weapons attack
RUN
HIDE
TELL

Powered by Urim, the ACT app is free for businesses and has been developed in partnership with industry specialists from Marks and Spencer and Highfield eLearning. Available from Google Play or App Store, the app will provide access to:

- Practical advice and guidance to help you protect your business, plus information on how to respond in the event of an attack.
- Information on Counter Terrorism Policing's suite of ACT training products, plus access to the online e-Learning package.
- Suite of National Counter Terrorism Security Office guidance videos.
- Latest reference documents and publications.
- ACT online reporting form and confidential hotline.
- Emergency response and post-incident guidance.
- Live-time news updates from UK Protect.