ProtectUK

Tactic DB3: Ensure that all visitors and contractors provide at least 24 hours' notice prior to attendance

ProtectUK publication date

14/12/2023

Information and Intention

In many organisations, the traditional approach to security has focused on addressing physical and information security issues. The people element, which is equally important, has often been overlooked. The actions and attitudes of people can make all the difference. A significant factor affecting how people act is the security culture of the organisation. This can be defined as the styles, approaches, and values that the organisation wishes to adopt towards security. In organisations with a strong security culture, employees will tend to think and act in a more security conscious manner, helping reduce risk and vulnerability, which in turn helps protect against reputational damage, business impact and ultimately national security threats.

Effective security measures can help to create a controlled environment which will encourage positive security behaviours amongst staff, visitors and contractors, act as a deterrent and protect from criminality, including terrorism. Therefore, all visitors and contractors accessing the premises should be required to provide at least 24 hours' notice prior to reporting to reception, or an individual in authority, who will escort them to the reception.

This process provides audit information, including sign-in/out times, the purpose of the visit, and can be crucial in the event of an emergency evacuation of the premises. Visitors and contractors should be given a security awareness briefing as well as a health and safety briefing as part of the personal risk assessment process.

Ensuring at least 24 hours' notice of arrival enables appropriate personnel screening, verification of vehicle, and preparation of visitor and vehicle passes. It is important that the organisation, where possible, conducts identity checks prior to the arrival of the visitor or contractor. It is essential that some form of identification check is carried out on individuals prior to attendance or employment.

These should be able to confirm an individual’s identity, employment status (where applicable), nationality, details of person they are visiting and purpose of visit.

Method

Visitors should sign-in and be issued a pre-prepared, individual visitor pass. If appropriate, a vehicle pass should also be issued. All visitors should have a legitimate reason for their visit. These identification passes should be worn and be visible at all times.

Anyone not wearing a pass or displaying a pass on their vehicle should be reminded by a member of staff of the security procedures and requested to present the identification. Failure to do so should be reported immediately to security/senior management. If safe to do so, the individual should not be left alone, or their vehicle left unattended. Visitors should be escorted at all times when not in public areas.
Visitors and contractors should be given a security and health and safety awareness briefing by an appropriately trained member of staff on arrival at the premises. This should include the following messages:

- Where an individual and vehicle pass is issued, it should be displayed prominently at all times while they and their vehicle are on the premises.
- Anyone without a pass or in an unauthorised area will be challenged.
- If a vehicle has been parked on-site, any work/parking permits should be displayed prominently in the windscreen and returned prior to leaving the site.
- To be vigilant when on the premises and what to do if they see a suspicious item or a person acting suspiciously.
- All doors should be properly closed when leaving, particularly doors leading to non-public areas.
- Tailgating into non-public areas should not be allowed.
- Worksites and equipment should be secured on leaving.
- Visitors and contractors have a duty of care for themselves and other staff members.

Administration

Policy and procedures should mention the requirement to ensure that all visitors and contractors provide at least 24 hours' notice prior to attendance, should the threat level be raised or following an incident. Identify ownership of the enhanced security procedure and governance of the decision making, including who is responsible for the management, coordination and strict compliance, together with the relevant record keeping, and how its effectiveness is assured. Ensure staff understand processes and procedures to be adopted, including action and contingencies.

Risk Assessment

Personnel/People Security is the responsibility of everyone, not just dedicated security officers or security personnel. It is essential that a clear message is communicated to all employees, instructing them to report reservations regarding visitors or contractors who are demonstrating behaviours of concern e.g. accessing work areas not related to their role for no apparent reason, or colleagues' equipment.

Three types of people and their roles need to be considered:

- Security personnel
- Front-line staff
- Members of the public – this concerns providing information and guidance to people visiting your site on how to protect themselves should an incident arise or to recognise an attack is underway. This can include various types of communication such as posters, announcements, signs etc.

A risk assessment should identify threats which could have an impact on the business and recognise any existing vulnerabilities. Risk assessments should clearly define a duty of care to staff and others on both an organisational and individual level. Staff and visitors may have different responses to the same incident and therefore you should risk manage the impact of staff, contractors and/or visitors, as well as members of the public, not following or directly contradicting instructions.

For more information, see ProtectUK - Security Risk Management.

Communications

Internal Stakeholder Engagement:

Certain aspects of security at your site may not necessarily be communicated to all your staff. However, staff members should be briefed on what to do should they observe suspicious activity, and they should be encouraged to identify and report any suspicious activity or item they observe, or that they know about.

It is necessary to ensure points of contact are known to staff internally, and partners externally. Any information regarding visitors and contractors requiring to provide 24 hours' notice, prior to attendance, should be disseminated internally through the communications function.

All security management/security staff should understand where security staff should be positioned and what the new procedures are. Internal communications should encourage security awareness by general staff and a positive security culture should be encouraged through internal communications.

You must provide information for your staff so that they can help deliver on the security plan. Your internal audience will inevitably cross over into your external audience, so consider what messages you want them to share with external networks, e.g. families and friends. Remember that social media is a potential area where this crossover may occur.

External Stakeholder Engagement:

Engagement with neighbouring businesses should include basic information regarding the security process if it impacts on neighbours. However, specific information on security procedures should not be shared externally.

Early identification and engagement with key external stakeholders are important. Local organisations whose sites are nearby, or have shared use of the site being protected, are also likely to play an important part in developing and delivering the plan, and consideration should be given to engaging with any working groups or fora who may already have identified 'best practices' and lessons learned from similar sites within the business area the site operates within.

There are a number of key principles that should be applied when engaging with stakeholders:

- The engagement should be different for different stakeholders, at different times – it should be flexible as one type of engagement process does not necessarily suit all stakeholders.
- It should be a two-way engagement process, where information and knowledge are shared.

- Communications should be genuine and timely, where there is the ability to influence outcomes, dependent on feedback.
- Engagement with stakeholders should be open and transparent.

As with all matters relating to security and policing, the relationships with the police are key. The contact may be with either the local police or those specifically tasked with providing policing to certain sites.

External Media Engagement:

Engagement with the media should be encouraged to allow a positive and deterrent message to be disseminated to the general public, as part of the Security-Minded Communications strategy. By positively reinforcing a security deterrence message, it is likely that this may deter potential attackers when they carry out online hostile reconnaissance as part of the attack planning process.

Health and Safety/Other Legal Issues

The protection of visitors at a location is governed by legislation, such as:

- The Disability Discrimination Act 1995
- The Human Rights Act 1998
- Health and Safety Acts
- The Data Protection Act 2018
- The Fire Safety Order 2005
- The Fire (Scotland) Act 2005

It is important to consider any change to security processes and/or activities with regards to justification, proportionality, necessity and legality.

You should ensure that there are well-defined governance arrangements and that records are kept of the issues, decisions made and the reasoning behind those decisions which involve security related to visitors and contractors. Records will provide evidence to any investigations, or public enquiries,

and assist in defending against legal action, criminal charges or civil claims. The importance of keeping accurate records and having well defined governance arrangements has been demonstrated during the Manchester Arena Inquiry.

Such changes that affect visitors, contractors and the organisation must include consideration of relevant legislation as well as details of your organisation’s insurance policies. Consideration must be given regarding the personal health and safety of security staff in the performance of their duties.

KEYWORDS
SECURITY
SECURITY CULTURE
RISK ASSESSMENT
EVENT SAFETY
VISITORS
IDENTIFICATION
ID BADGES