ProtectUK

Tactic DB6: Ensure all staff are challenged and their ID checked

ProtectUK publication date
14/12/2023

Information and Intention

It is important to ensure that a site is kept secure while remaining accessible to your visitors or customers. All staff and visitors should wear ID badges/passes while they are at your premises. This is to ensure that staff are able to identify who works at your business and who is visiting your business, and to ensure that they only have access to the parts of your business that are necessary for them.

There will be areas in a site or venue that, for various reasons, should be kept closed to the public. The public and private areas should be clearly marked, with appropriate access control measures in place. To be effective, any system requires active management, appropriately trained staff and a good security culture.

Method

Identification passes should be issued to staff and visitors and always worn whilst on site. Staff should wear their IDs and be made aware of the role and operation of the access control system or policy. Staff training should include actions to take:

- If a pass is lost or stolen;
- If a person needs to be challenged;
- In response to suspicious behaviour.

Reception areas can provide a focal point for visitors to report to before entry, enabling credentials to be checked and authorised visitors to be booked into the building. Visitors should sign-in, be issued visitor passes and have a legitimate reason for their visit, as well as a sponsor (who will be responsible for the visitor while they are in your buildings, including escorting). These identification passes should be worn and ‘be visible’ at all times, anyone not wearing a pass should be asked by a member of staff why they are not wearing a pass. Consideration should be given to whether visitor passes can be clearly distinguished from staff badges. All passes should be returned to the reception or a specified person before leaving the site.

Photo passes should be mandatory for contract and agency staff. These should be worn at all times whilst on site. The employing organisation should retain contractors’ passes between visits, reissuing them each time, but only after the contractor’s identity has been verified. An expiry date should be visible on the pass.

Both visitors and contractors should be given a security awareness briefing.

An effective access control policy or system should include adequate training of staff and should highlight how to overcome bad practice such as tailgating and holding doors open, as well as the promotion of a good security culture. Staff should feel safe and empowered to challenge or report suspicions.

Questions that security managers and leadership at businesses should ask include:

- Does your organisation have clearly defined access control guidelines or policies? If so, who owns them?
- Where are the access points in your organisation (staff, visitors and vehicles)? How are they monitored and protected? How does access control differ for different people: staff (are they pass holders), visitors (is security clearance needed), people making deliveries?
- Are there areas requiring greater or fewer security requirements (secure and non-secure areas)?
- How are security passes and clearances processed, and what checks are required?
- Do staff know what all passes look like?
- Who is responsible for issuing passes, enforcing the wearing of staff and visitor IDs, and collecting IDs when visitors are leaving the sites?
- Are there clear communications to staff on the reasons why wearing ID passes is important and highlighting the need to challenge those that are not wearing them?

Administration

There should be clear policies and procedures for how access control will be used and operated. Similarly, clear policies on the issuing and wearing of staff and visitor IDs should be created and communicated effectively.

Ownership should rest with the leadership at the business, the security manager or those responsible for security and safety.

Consideration should be given to how misuse of the system by staff, visitors and customers will be challenged. There should also be a policy for the surrendering of passes for both permanent and contracted staff, either once the member of staff leaves their employment or the contracted period ends. The sponsor of the visitor should be responsible for ensuring the visitor pass is returned at the end of their visit.

Risk Assessment

All activity relating to access control and staff ID should be risk assessed in line with existing business/organisational policies.

The creation of a Crisis Communication Plan (TACTIC EB4) should be a core component of your risk preparations. This should be developed following a detailed risk analysis looking at potential issues and possible solutions. This plan should be aligned with operations within the business, such as access control, as well as key decision makers.

Communications

Internal Stakeholder Engagement:

To be effective, any policy or system requires active management, appropriately trained staff and a good security culture. Internal communications play a vital role in helping achieve the best security behaviours amongst staff. Visual communication through posters, emails, or other media can influence behaviour.

You must provide regular information for your staff so that they can help deliver on the security plan. Use existing staff communication channels, such as shift briefings and the intranet, to inform your staff what suspicious activity may look like. Encourage them to trust their instincts and report anything suspicious immediately to management, security staff, or the police. In these communications, reinforce the message that reports will be taken seriously and be investigated. Where possible, highlight examples where previous staff reporting has led to positive outcomes; this helps promote confidence.

External Stakeholder Engagement:

Access control measures are a strong indicator of the security regime on a site and should be complimented with clear signage for customers and those external to the organisation.

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

Ensure compliance with the requirements of Health and Safety and other legal issues, such as:

- The Human Rights Act 1998
- Health and Safety Acts
- The Disability Discrimination Act 1995
- The Data Protection Act 2018
- Employment Rights Act 1996
- The Fire Safety Order 2005
- The Fire (Scotland) Act 2005

Your actions must be justified, necessary and proportionate to the threat you are facing.

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 closure of non-

essential access and egress. 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.

Security positioning and patrolling 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
EVENT SECURITY
ACCESS CONTROL
STAFF
SECURITY MINDEDNESS