ProtectUK

Access control

Original publication date
02/11/2020

1. Introduction

It is important to ensure that a site is kept secure while remaining accessible to your visitors or customers. 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. Measures at crowded places will differ depending on the conditions of entry. To be effective, any system requires active management, appropriately trained staff and a good security culture.

Access Control Checklist

2. Appearance

The access control system is a strong indicator of the security regime on a site and should be complimented with clear signage. A challenge culture by staff will also deter hostile reconnaissance. However, consider balancing the deterrent effect of appropriate signage with the possible assistance being given to an adversary carrying out hostile reconnaissance.

Go to the NPSA (formerly CPNI) Control of Access webpage to learn about keeping a site secure.

3. Operational requirements

When planning your access control system, first carry out a risk assessment and conduct an Operational Requirement (OR). This will assist with the identification of the problem needing to be solved and the most appropriate solution.

Go to the NPSA Operational Requirements webpage for the latest guidance in this area.

4. Ease of access

Examine the layout of the site and access control system. Make sure that the entry and exit procedures allow legitimate users to pass without too much effort or delay. Consider how your access control system will work in busy areas at peak times. Access measures should be appropriate for the site and not be unnecessarily onerous.

Go to the NPSA Access Control and Locks webpage to find out about technology and control systems.

5. Policy and procedure

There should be clear policies and procedures for how the access control system will be used and operated. Consideration should be given to how misuse of the system by staff, visitors and customers will be challenged. Staff should feel empowered to challenge anyone entering an area without the correct pass, or who looks in any way suspicious.

6. Training

Make sure staff are aware of the role and operation of the access control system. If you have any access control equipment in place, the installer should provide adequate training. Training should include the action to take:

- if a pass is lost or stolen
- if a person needs to be challenged
- in response to suspicious behaviour

7. Security culture

An effective access control 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 to challenge or report suspicions.

Go to the NPSA Security Culture webpage to learn more about supporting a strong security culture.

8. System maintenance

The system should be regularly maintained and kept in good working order. The installer should supply all relevant system documentation, for example log books and service schedules. Be aware of the actions required in the event of a system failure. System failures must be dealt with immediately and a contingency plan put into place. This may be to secure a door, or provide a security officer at the point of failure, with all actions being recorded. A make sure suitable maintenance agreement should be in place which will rectify problems quickly (Service Level Agreement).

9. Manual access control

If after carrying out the OR, a decision is made that a manual locking system is appropriate, there should be a robust management process in place incorporating the following:

9.1 Key management

Key management is crucial in order to maintain the integrity of the system. A record of all keys issued and conduct regular audits should be done. All keys issued should be returned as part of the exit procedure for staff leaving the organisation. If a key cannot be accounted for, there should be a contingency plan to deal with a potential compromise of access control.

9.2 Additional management control systems

An electronic lock may be appropriate. This offers a compromise between mechanical locks and a fully electronic access control system. If mechanical PIN code locks are used, a plan should be in place to change PIN codes regularly. Best practice is to change them after a member of staff leaves, after a security breach or every 6 months.

10. Integration

The access control system should support other security measures. Consider system compatibility between access control, alarms, CCTV and text alert systems.

Go to the NPSA Physical Security webpage to learn about keeping your buildings and sites secure.

10.1 Compliance

The access control system should be compliant with:

- the Equality Act 2010
- the Human Rights Act 1998
- the Health and Safety at Work Act 1974
- the Data Protection Act 1998 (superseded by the General Data Protection Regulation (GDPR) and Data Protection Act 2018 in May 2018)
- the Regulatory Reform (Fire Safety) Order 2005
- the Fire (Scotland) Act 2005

The access control system will have a set response to fire alarms, for example doors that automatically unlock when an alarm sounds. For critical areas such as control rooms, fail-safe systems must be compliant with both health and safety and security requirements. Make sure that when an access control system is specified, consideration is given to what areas may remain locked in an emergency, as security should never compromise safety. Procedures should be in place to maintain the integrity of any sensitive assets in the event of an emergency.

11. Lockdown procedures

Due to the potential for firearms or weapons attacks, or protest activity for example, it is important to consider the option of implementing a dynamic lockdown procedure. Seriously consider how your access control system aids or hinders this. There may be features in the access control system that

can be used during a lockdown. These features should be quick and simple to activate and staff should be trained in their operation.

Read more about evacuation invacuation, dynamic Lockdown and protected spaces.

12. Vetting procedures

Consideration should be given to how vetting procedures impact access control. A decision regarding staff access to all areas, or whether there are restricted areas to the site. Staff and visitors should only be given access to the areas required for their role. Passes may vary in type, depending on the area accessed.

The manager of the access control system has a critical role. Only this person or their deputy should issue passes. Passes must be signed for once the identity of the recipient has been confirmed. Out of hours, the security supervisor may be authorised to issue temporary passes, but this should be by exception and any visitor should be escorted. Any temporary passes issued must be of limited duration.

13. Search procedures

If the OR identified that searching is necessary at the site, then there are a number of things to consider. The primary consideration relates to the nature of the threat faced. Identify the aim of the search and the type of items being searched for. Appropriately trained staff should be used, plus well-maintained equipment and sufficient space and a suitable environment to conduct the search.

Read more about Search Planning to learn about reducing the likelihood of threats entering your building or site.

14. Vehicle procedures

If the OR identifies the need for vehicular access control, then there are a number of things to consider. Search procedures must be consistent with the threat. The ideal solution is to restrict the number of vehicles accessing the site and any search should be conducted as far away as is reasonably practicable. Ideally, access will be afforded only to vehicles that are booked in and expected, with the identity of the vehicle occupants confirmed.

14.1 Vehicle access passes

Certain vehicles may need to routinely access your site. It may be prudent to issue vehicle passes to identify vehicles and the management of these passes should be commensurate with all the other access control measures in place. Vehicles that need to gain access without a pass should only do so by prior arrangement.

14.2 Automatic Number Plate Recognition (ANPR)

Automatic Number Plate Recognition (ANPR) may be a useful addition to an integrated security regime, but will only provide information related to a registration plate and should not be solely relied on. Any data or information that can lead to the identification of an individual should be stored in accordance with the GDPR.

15. Increased threat

At times of increased threat, further access control measures may be required for staff, vehicles, or both. This should be reflected in the site security plan. Vehicle access control may be enhanced by the application of Hostile Vehicle Mitigation (HVM).

Read more about threat level and building response plans to better understand the threats your building or site might face.

16. Summary

The OR process is fundamental to planning an efficient security solution and access control is no exception; whether controlling pedestrian or vehicle access into a site, the principles are the same. Individuals should know who and what is allowed to go where and allocate passes to reflect this, with access suitably limited.
Any access control system is only as good as the procedures and the people that govern its use, and a good security culture is paramount in making sure your site remains secure.

KEYWORDS

ACCESS CONTROL

HOSTILE RECONNAISSANCE

SECURITY CULTURE

PUBLICLY ACCESSIBLE PLACES

PALS GUIDANCE

PALS

PUBLICLY ACCESSIBLE LOCATIONS