Good Practice Guide

Basic Physical Security Fit-out for Zones 1 & 2 (Front-of-House)

This guide contains practical physical fit-out suggestions government organisations can use to mitigate the risk of customer-initiated violence in front-of-house service delivery spaces (i.e. Zones 1 and 2 primarily for interacting with customers).

Overview

This guidance is designed to assist when considering the risk of customer-initiated violence as part of acquiring new sites or upgrading existing facilities and covers the following components:

1 Access

1.1 Managing access

1.2 Entry restrictions

1.3 Emergency egress

1.4 Doors

1.5 Electronic Access Control Systems (EACS)

1.6 Reception counters

1.7 Elevators and stairs

2 Facilities

2.1 Service delivery desks

2.2 Meeting rooms and interview rooms

2.3 Toilets

2.4 Fixtures and fittings

2.5 Secure glazing

2.6 Car parking security

2.7 Deliveries and loading bays

3 Equipment

3.1 Duress alarms

3.2 Identification

3.3 Screening and x-rays

3.4 Security lighting

3.5 Surveillance and loitering

3.6 Perimeter security

4 Assurance

4.1 Using security guards

4.2 Drills and testing

4.3 Local environment

Site selection, building and service design

Assessing the risk of customer initiated violence in new or upgraded facilities should be part of a broad risk approach, which means thinking about the root cause of any harmful event, the likelihood it will occur and the consequences if it does. See WorkSafe New Zealand's position on Risk Management at Work, which provides a helpful overview of what you should focus on when managing risk and how you should manage risk as a duty holder.

The duty to undertake regular risk assessment may also compel you to address issues as they become apparent, including risks and issues that are raised by customers, and workers and their representatives.

To mitigate the risk of customer-initiated violence in front-of-house service delivery spaces, you should consider the following good practices:

- ensure contractual arrangements you enter into for a particular site support your ability to manage your particular security needs effectively; this is particularly important when it comes to co-locating or taking up occupancy in a site with multiple tenants
- consider the duty to collaborate, cooperate and consult with other people conducting a business or undertaking (PCBUs) to manage risk
- ensure you have considered the local community and the broader environment of the location in terms of the particular risks associated with that local community and factor these risks into your thinking
- consider customer-initiated violence before committing to a co-location; this requires conversations about security with potential co-located agencies and satisfying yourself there is a good, combined view on managing security and service delivery in the co-located space.

Taking an integrated approach to security

When thinking about security at a particular workplace or set of workplaces, you should use an integrated approach that considers the design and delivery of services alongside the physical fit-out and design of your workplace.

If you've identified and assessed a hazard as significant, it must be controlled using the hierarchy of controls. See WorkSafe New Zealand's how to

manage work risks using formal risk assessment and management processes (including the duty to eliminate or minimise risks).

A significant hazard should be eliminated, if it can't then isolated, and if that isn't practicable, controls should be put in place to minimise the hazard. If it is not a significant hazard you must still take all practicable steps to ensure the equipment is safe for workers to use.

To achieve an integrated approach, within a hierarchy of controls analysis, you should think about the following good practices:

- good service design can go a long way to offsetting the risk of customer-initiated violence; consider how the design of your services can enhance security and eliminate aspects of your service model that create unnecessary security risks
- good service delivery can also help offset the risk of customer-initiated violence; for example, you might consider whether:
    - front-line workers have the skills and support needed to deliver your services effectively and securely
    - front-line workers have the right training and other support needed for effective and secure service delivery
    - you are effectively monitoring performance and can adjust based on these learnings
    - you have the policies and procedures needed to enable workers to conduct themselves in a safe and secure manner
- understand your customer's experience; use customer insights to identify and remove stressors such as unnecessary queuing or delays; try to design services that empower customers to help themselves
- when thinking about security and the customer experience, try to ensure workplace security is unobtrusive and does not unnecessarily impede the customer's service experience; government services must be secure and safe but they must also remain open and accessible as far as practicable
- while the physical technology may remain unobtrusive, you will need to consider ensuring customers are aware of certain security measures such as CCTV monitoring; you may, for example, put up prominent signage warning customers that they are being filmed.

1 *Access*

1.1 Managing access

When thinking about managing how customers access your front-of-house service spaces, you might want to also consider the following good practices:

- separate your initial reception areas from service delivery with access into the service delivery space
- use your reception point as a delivery point for simple, transactional activities such as providing generic information or leaflets; as far as possible, try to keep the number of customers in the service delivery space to only those who need specific services and support from staff
- have controlled barriers such as electronically-activated barrier doors or turnstiles to manage access into your front-of-house spaces
- if you use barrier doors or turnstiles, consider how customers gain access, for example:
    - workers monitoring the doors or turnstiles should have discretely located remote door-release mechanisms
    - if the release mechanisms are behind the barrier door then you will need to consider things like:
        - staff line of sight
        - closed circuit television (CCTV) monitoring the space
        - buzzers or telecoms for customers (these may be particularly useful when staff are not necessarily actively monitoring the door)
    - use security officers to monitor people entering the facility and controlling the barrier doors/turn-styles
- ensure customers cannot easily access areas where non-front-of-house workers are located (i.e. office space) or other security zones.

Accordingly, security doors and other strict access controls should be used to protect these areas.

1.2 Entry restrictions

When thinking about how and when to restrict entry into a front-facing service space, you should consider the following good practice:

- restrict access for individuals who represent a direct and immediate threat to safety and security while ensuring customers have continued access to services without unnecessary impediment or hassle

- have a clear statement or policy on the grounds for restricting access to front-of-house service space (and how this will actually be communicated).
- ensure gang insignia is prohibited; the Prohibition of Gang Insignia in Government Premises Act 2013 prohibits the display of gang insignia in any government premises; accordingly, all government organisations should have policies preventing persons displaying gang insignia (with sensible judgments around tattoos) from entering government workplaces
- have a clear policy position on restricting access to:
    - customers that are clearly intoxicated
    - customers who are hostile or aggressive
    - customers subject to a trespass order or harassment order (or similar legal remedy)
- have a clear policy and set of procedures for sharing information about an individual who is subject to trespass order or harassment order
- have a clear policy and set of procedures and processes for removing customers causing problems in the workplace
- your policy may also want to reference how, why, and when a facility might be locked down in an emergency
- have a clear set of alternative service delivery mechanisms for delivering services to customers denied access to service areas; you might want to consider options such as:
    - online service delivery
    - specialist high-risk customer service delivery
    - alternative arrangements such as proxies/agents acting on behalf of high-risk customers.

1.3 Emergency egress

When planning how workers can withdraw from or evacuate a space during an emergency or hostile situation, you will need to address how your front-line workers will deal with their own safety and that of customers and visitors who may be bystanders during an event.

This is particularly important if, for example, your immediate withdrawal planning focuses on workers retreating to more secure, worker-only locations.

For workers, such as receptionists, who are likely to be the first point of contact for a disgruntled or fixated individual, it is good practice to have some sort of safe withdrawal exit system.

1.4 Doors

When thinking about how people move into and out of your workplace, doors are a critical aspect of your overall security design. You should consider the following good practices:

- any solid doors should have a glazed panel; this helps minimise the health and safety risk of people having doors opened suddenly on them; glazing also helps people to ensure it is safe to open the door
- electronically lockable or physically locked doors should allow egress at all times by use of a lever only (i.e. there is easy emergency egress)
- all outward facing doors should have robust hinge protection to increase resistance to forced entry
- all doors between zones should have automatic closing mechanisms
- there should be alarms that will alert when doors have been left open (e.g. longer than 20-30 seconds)
- all doors should have emergency release switches that are clearly marked and your Electronic Access Control Systems (EACS) should also have some sort of emergency locking over-ride
- reception over-ride should provide reception workers the ability to allow and prevent access, discretely
- emergency doors should fail to unlock (fail safe – means door allows unrestricted egress without swipe)
- exterior doors should fail safe and fail secure (i.e. unlocked from the inside but remain locked from the outside)
- all exterior doors with fail secure mechanisms should have systems in place for allowing easy Fire Service override)
- you should not use low security doors such as glass sliding doors in transition areas between Zone 1, fully public areas, and any controlled zones.

1.5 Electronic Access Control Systems (EACS)

You should have an effective and appropriate EACS implemented at any front-facing site. This EACS should prevent members of the public from accessing controlled areas while allowing workers located in the front-of-house area to escape

emergencies easily. You should consider the following good practices:

- ensure your EACS complies with the NZSIS's Information Security Manual (NZISM)
- strict controls over the system including change control; your Chief Security Officer (CSO) should have exclusive authority over the EACS
- systems to ensure things such as Access Cards are managed (i.e. cancelling lapsed cards, return policies, having the ability to use a security matrix to align cards to clearance levels)
- a regular system of check-ups, tests, and drills to ensure the equipment works, is actively maintained, and works in the way anticipated (i.e. in accordance with emergency plans).

1.6 Reception counters

When thinking about the design and layout of reception desks, you should consider the following:

- design reception desks to prevent customers from being able to jump desks. This could include:
  - no footholds or ability to step up from the customer's side
  - discrete bands of glazing or wires
  - a suitable height to limit the ability to scale and gap to ceiling
  - avoiding hand grips (use big rounded edges that make getting hold difficult)
- design desks so that customers cannot easily reach, stab, grab or punch workers
- whether the reception desk is located alongside the service delivery area (i.e. inside barrier doors) or outside of the service delivery area.

1.7 Elevators and Stairs

When considering a tenancy or building design, you might want to ensure elevators and stairs are effectively secured. This could include the following good practices:

- ensure elevators and stairs are controlled using EACS so that customers and other tenants cannot access controlled areas such as Zones 2, 3, 4, or 5 via elevators or stairs
- have clear policies about secure movements such as no tailgating, worker awareness (stair-dancers etc.)
- ensure your operations and service areas are appropriately secure from other tenants (through EACS).

2 Facilities

2.1 Service delivery desks

When thinking about the service delivery desks you should consider the following good practices:

- desks used for customer service should be sufficiently large to prevent being picked up easily; a good practice suggestion is no less than 1750 mm in length and 900 mm in width OR anchored
- if a room cannot fit a 1750 mm desk then the desk should be the full width of the room and anchored to the walls or floor.

2.2 Meeting rooms and interview rooms

When designing meeting rooms and interview rooms where your workers may interact with customers, you should ensure workers are secure in these smaller spaces by considering the following good practices:

- how customers access/egress the room, such as:
  - having EACS on the public side of the room controlling access into the room so customers cannot enter the room without a worker's knowledge
  - ensuring unfettered emergency egress is maintained
  - an automatic door closer.
- Meeting and interview rooms should have sufficient glazing to enable clear surveillance of room while also preserving the dignity and privacy of the customer interaction.
- Meeting and interview rooms should be sufficiently sound proofed to enable workers outside of the room to hear heated discussions or yelling. However, the soundproofing should be sufficient to preserve the dignity and privacy of the customer interaction.
- Tables in meeting rooms should be configured according to risk profile.
- Tables and customer chairs in interview rooms should be discretely secured to the floor.
- Worker's chairs in interview rooms should have wheels to allow rapid withdrawal.
- Duress alarms should be fitted in all interview rooms in such locations to enable workers to activate the alarm easily and discretely.

You might also want to consider duress alarms in meeting rooms based on the risk/threat profile.

2.3 Toilets

When thinking about toilets in front-of-house spaces, you might want to consider the following good practices:

- members of the public should not have access to any toilet facilities in restricted areas
- workers in the public area should have clear line of site of the toilets to enable them to monitor who goes in and comes out of toilets (to prevent the risk of customers hiding in the toilets)
- if you have public toilet facilities, workers should not use those toilets
- if toilets are not provided in the public space, you should have a prepared response that directs members of the public to the nearest toilets.

2.4 Fixtures and fittings

When thinking about the security of fixtures and fittings in public spaces, you will want those fixtures and fittings to support a professional, comfortable, welcoming, and practical environment but to be secure (i.e. not easily used as weapons). You might want to consider the following good practices:

- discrete anchoring of fixtures and fittings (e.g. anchoring waiting space seating)
- clear policies about clutter and eliminate unnecessary items that could be used as weapons from public spaces (if you are going to have objects like staplers in the public space, you might want to have policies to ensure they are kept out of easy reach of customers).

2.5 Secure glazing

In areas where the public area (zone 1) transitions to a more secure/controlled area, you might want to consider glazing.

Sites with elevated risk of violent or aggressive client behaviour must have security treatment to all glazing that forms part of the controlled zone perimeter, such as laminated glass and security film.

2.6 Car parking security

If your workplace has worker car parking, you should consider the following good practices:

- workers should be able to move from their place of work to onsite carparks as directly as possible
- carparks must be well-lit at all times (and/or supported by activator switches)
- hiding places such as shrubs or recesses or other shielding that could hide a person should not be near carparks
- worker parks must not be marked with designations (e.g. “Manager’s Park”)
- visitor parks should be clearly marked
- visitor parks should be observable from the office
- car parking drives and roadways should not be near entrances. If car parking drives and roadways are near entrances, bollards should be contemplated.

2.7 Deliveries and loading bays

To secure delivery areas and loading bays in your workspace, you should consider the following good practices:

- restrict deliveries to a specific designated place and locate that delivery place to maximise security
- ensure mailrooms and loading bays are separate from business operations
- CCTV should be positioned to identify delivery personnel
- delivery counters should include suitable partitions that can be secured after a delivery.

3 Equipment

3.1 Duress alarms

When thinking about duress alarm systems for your front-of-house workers, you should consider the following good practices:

- ensure activators are hard wired in discrete locations; you should ensure the location and number of activators is informed by providing your staff with the ability to discretely activate alarms without the customer’s knowledge in all of the expected interactions
- duress alarms will need policies and procedures making it clear how and when people respond to duress alarms; duress alarms should be integrated into the security system
- where there are multiple activators, have a system to identify which particular activator has been activated
- duress alarm activation should trigger an unmissable signal to others such as a strobe light and/or sounders
- strobes and alarms should not be heard or seen by public but they should be located in places that reliably alert staff of a problem.

Duress systems need to be tested and maintained regularly. Testing should include activation and response.

3.2 Identification

When controlling access in and around your workplace and to ensure only authorised people have access to certain areas you should consider the following good practices:

- use worker ID cards that are clearly visible at all times
- contractors and other authorised visitors should also have visible identification; you may need to have policies and procedures in place to ensure people with different clearances/profiles have appropriately managed movements (i.e. contractors may not go into certain areas unaccompanied or workers with certain clearances may go certain places)
- workers should be encouraged to hide identification when outside of the workplace, especially when there is a direct threat against your worker(s) or agency.

3.3 Screening and x-rays

Searching and screening customers is generally unnecessary and unsuitable for most government functions. If you are considering searching and screening arrangements you will need to consider the legal implications first. It is therefore good practice to discuss with your agency's legal advisers, any arrangements that relate to searching or screening of customers, prior to initiation.

3.4 Security lighting

When you are thinking about the security lighting of your workplace, you should consider the following good practices (which may also be a shared responsibility with other 'people conducting a business or an undertaking' (PCBUs):

- ensure all areas immediately outside of workplaces are well lit, including worker carparks; a good guide for lighting levels in particular situations is the Australian/New Zealand Standards for Interior and Workplace Lighting, particularly section 5 Outdoor Workplace Lighting (2012) AS/NZS 1680.5: 2012. At a minimum, you should consider how you illuminate:
    - large, open exterior areas
    - exit points
    - exterior locations where people could potentially hide or loiter
    - worker car parking areas - including entrances and exits to carparks and ensuring sufficient lighting to ensure there are no blind spots between vehicles and clear lighting between exit points and car parking
    - walkways
    - stairwells
    - external equipment stores
- consider the use of motion sensors
- consider the interaction of lighting with any external surveillance (e.g. CCTV); you should consider the impact of glare and other lighting effects when thinking about the location of lights and surveillance
- consider many smaller lights rather than fewer more powerful lights.

3.5 Surveillance and loitering

Ensure your front-of-house spaces enable effective surveillance so that worker interaction with the public is observable both directly and indirectly. You should consider the following good practices:

- identify and eliminate all hiding areas (curtains, corners, recesses, etc.)
- ensure areas where customers and workers interact are clearly observable through clear lines of site
- put glazing on all doors and meeting rooms to enable workers to observe
- use CCTV to help maintain surveillance; if you use CCTV you will need to consider how screens are monitored and what actions are taken by whom in response to an incident on the CCTV; you should also think about whether you will record CCTV footage, the periodicity of overwriting recorded content and/or how long you will store recorded footage
- have systems and processes in place to enable you to monitor your exterior or perimeter areas (e.g. observe loitering)
- if part of a multiple tenancy, you might want to consider arrangements to monitor loitering and notification of suspicious people.

3.6 Perimeter security

When you are considering perimeter security of your workplace, you should consider the following good practices:

- a minimal number of potential entries into the site
- emergency exit doors, which should generally be only used for emergency exit

- controlled areas such as worker-only areas and worker-only exits, which should be obscured from casual public view
- perimeters which are kept clean and tidy and periodic sweeps to ensure there is nothing that can be used to force entry or picked up and used as a weapon
- in shared tenancy arrangements, you may need to talk to landlord/lead tenant to ensure perimeters are kept tidy and secure.

4 Assurance

4.1 Using security guards

When you are thinking about whether to use security guards at barrier entrance points, you might want to consider the following good practices:

- ensure security guards actually help your security; you might, for example, consider:
    - the limited powers of security guards
    - the customer experience (and the message guards on door duty sends)
    - what is reasonably practicable to protect people from harm
    - using security guards as a temporary response to high risk, with clear review periods.

  NOTE: It is only after assessing the extent of the risk and the available ways of eliminating or minimising the risk that consideration may be given to whether the cost associated with available ways of eliminating or minimising the risk is grossly disproportionate to the risk.
- ensure you are clear about how you intend to use security guards
- think about the health and safety consequences of having security guards in your workplace and how you are managing your contracting obligations.

4.2 Drills and testing

When thinking about maintaining security in your front-of-house spaces, you should consider the following good practices:

- a regular schedule of testing conducted by competent, qualified testers; testing should not only test that the equipment works but that it also works in the way that it is intended (i.e. testing processes and procedures)
- regular drills to ensure your policies and procedures work and your workers know what to do in different situations.

4.3 Local environment

As occupants of a particular site, your workers should monitor the local environmental context of their work to determine changes in threat levels. You may want to consider the following good practices:

- a system/process for monitoring graffiti and vandalism to your premises
- conduct regular meetings with community leaders
- undertake discussions with neighbouring building tenants/owners, other similar agencies and local Police
- a system for recording incidents and observations and feeding these into your security risk assessment processes.