PSR | Protective Security Requirements

Policy Version: 1.0 ***Last Review Date: Oct 2025***

Protective Security Requirements (PSR) Policy Framework:

PHYSICAL SECURITY (PHYSEC)

APPENDICES

Table of Contents

APPENDIX A: SITE SELECTION EVALUATION CRITERIA 4

APPENDIX B: WHAT TO INCLUDE IN A SITE SECURITY PLAN 6

APPENDIX C: PSR SECURITY ZONE REQUIREMENTS 7

APPENDIX D: ACHIEVING SECURITY IN DEPTH 12

APPENDIX E: GOOD PRACTICE PHYSICAL SECURITY DESIGN PRACTICES 15

- DETER, DETECT, DELAY, RESPOND, RECOVER 15
- CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN 15

APPENDIX F: RELEVANT STANDARDS FOR DESIGN OF PHYSICAL SECURITY MEASURES . 17

- STANDARDS 17
- HANDBOOKS/GUIDES 18
- CODES 18
- GUIDANCE FOR CONSTRUCTING PSR SECURITY ZONES 18

APPENDIX G: EVENT SECURITY 19

- BEFORE THE EVENT 19
- DURING THE EVENT 24
- AFTER THE EVENT 28

APPENDIX H: PHYSICAL SECURITY FOR ICT SYSTEMS 30

- INTRODUCTION TO PHYSICAL SECURITY FOR ICT SYSTEMS 30
- OUTSOURCED ICT FACILITIES 30
- SECURE YOUR ICT EQUIPMENT 31
- SECURE YOUR ICT SYSTEM EQUIPMENT 33
- PREPARE FOR DISASTERS 35
- SECURE YOUR ICT FACILITIES 37

APPENDIX I: SECURELY TRANSPORTING SENSITIVE ITEMS 40

- 1. ASSESSING THE RISKS 40
- 2. PLANNING SECURITY FOR THE ITEM 40
- 3. MANAGING THE ITEM'S SECURITY DURING TRAVEL 41
- 4. CONFIRMING THE ITEM'S SAFE ARRIVAL AND WRAPPING UP THE PROCESS 42
- BEST PRACTICE GUIDELINES FOR TRANSPORTING SENSITIVE ITEMS 42

APPENDIX J: SPECIFIC SECURITY MEASURES 46

- PERIMETER SECURITY CONTROLS 46
- BUILDING CONSTRUCTION 47
- ALARM SYSTEMS 49
- INDIVIDUAL ALARM OPTIONS 52

ACCESS CONTROL SYSTEMS 54

ALARM SYSTEM AND OTHER BUILDING MANAGEMENT SYSTEMS INTEROPERABILITY 57

LOCKS, KEY SYSTEMS, AND DOORS 57

CLOSED-CIRCUIT TELEVISION 62

SECURITY CONTAINERS AND CABINETS 64

SECURE ROOMS, SAFES, AND VAULTS 66

VISITOR CONTROL 67

RECEPTIONISTS AND GUARDS 71

OTHER PHYSICAL SECURITY MEASURES 72

Appendix A: Site selection evaluation criteria

Does the neighbourhood pose any risks?

Examples of neighbourhood-related issues that might affect the organisation's decision to use a site are the:

- level and type of criminal activity in the area
- impact of risks to or from neighbours (organisations, businesses, and residents)
- impact from over-sight of the organisation's operations
- suitability of staff access and safety after hours e.g., lighting
- proximity to sites which could become a target or attract large gatherings.

Is there enough space for a standoff perimeter?

The organisation may need a certain standoff distance to protect a building from threats. In some urban environments, it can be hard to achieve an effective standoff distance.

Remember to consider any threats pedestrians and vehicles may cause.

Does the site meet the organisation's access and parking needs?

Check and evaluate access through the standoff perimeter and into the facility.

- What is access like for pedestrian traffic, delivery vehicles, and cars?
- Does the site easily accommodate normal business?
- How will you control and monitor parking within the perimeter?
- Is the lighting suitable for safety?

Can all access points be secured?

Make sure all building access points can be secured, including:

- pedestrian entries and exits (including emergency or infrequently used doors)
- vehicle entries and exits
- air intakes and outlets
- service ducts
- windows
- roof.

Does the site accommodate the organisation's security zones?

Can the site provide the security zones needed?

Can security in depth be implemented at the site?

Will the site floor loading accommodate all the required security measures including:

- security containers and shelving
- wall construction.

Is the site at risk in a natural disaster?

Seek specialist advice about the risks of natural disasters in the area, and which mitigation strategies to apply. Contact local territorial authority for information on natural hazards for a site.

If the organisation chooses a site that is at risk from a natural disaster, select security products that help mitigate against the associated physical security risks if the natural disaster occurs.

What business continuity plan would you require?

Can the site support operations in a services failure?

Does the site cater for power redundancy if the site requires continual operation?

Have you undertaken due diligence on supply chain as defined in GOV5?

The site owner, building management, or other suppliers involved in the site could pose a risk to the organisation and due diligence must be undertaken as defined in GOV5 before considering the site for selection.

Appendix B: What to include in a site security plan

A site security plan documents measures required to counter identified risks to your organisations functions and resources at the site and articulates how the site-specific security elements work together to form the required security in depth. It also explains the reasoning for security controls chosen.

In your plan, document the answers to the following groups of questions.

Contact NZSIS PHYSEC for a typical site security plan template.

Location and ownership

What is the location and nature of the site?

Does your organisation have sole or shared ownership, or tenancy of the site?

People

What hours will your people work at the site?

Who else will visit the site (for example, the public, service providers)?

Who else will visit the site on behalf of the landlord (e.g., lift technician, building maintenance, window washers, cleaners)

What hours are you open to the public or other visitors?

Are there specific areas that need to be locked from general access at specific times?

Protectively-marked information

What protectively-marked information will be stored, handled, processed, or otherwise used in each part of the site? Which protective measures will you need for that information?

What security zones are required?

Which protective measures are needed for sensitive discussions and meetings (including those that involve protectively-marked information)?

ICT assets and resources

Which information and communications technology (ICT) assets and resources will be on the site? (Including, but not limited to, data, software, hardware, workstations, servers, frames and cabling, and portable devices such as laptops and tablets.)

Whole site, areas within the site, scalable measures

Which protective measures are needed for the site as a whole?

Which protective measures are needed for certain areas or zones within the site? For example, part of a floor that will hold information of a higher classification than the rest of the site.

How will you scale your security measures to meet increases in threat levels?

How will you secure the site in a disaster scenario (e.g., sustained power outage)?

Appendix C: PSR Security Zone Requirements

Zone 1 - Public access areas

These are unsecured areas including out-of-office working arrangements. They provide limited access controls to information and physical assets where any loss would result in a **low to medium** business impact. They also provide limited protection for people.

Examples of public access areas are:

- building perimeters and public foyers
- interview and front-desk areas
- temporary out-of-office work areas where the agency has no control over access.
- field work, including most vehicle-based work
- public access parts within multi-building facilities (for example cafes or shops).

In zone 1, you can:

- store information and physical assets needed to do business with low-to-medium BILs
- use information and physical assets with a **high or very high** BIL (storage is not recommended but is permitted if unavoidable)
- use information and physical assets with a BIL above **very high** only under exceptional circumstances with approval of the originating agency (no storage is permitted).

Zone 2 - Work Areas

These are low-security areas with some controls. They provide access controls to information and physical assets where any loss would result in a business impact up to **very high**. They also provide some protection for people.

Zone 2 areas allow unrestricted access for your people and contractors. Public or visitor access is restricted.

Examples of work areas are:

- normal office environments
- normal out-of-office or home-based worksites where you can control access to areas used for your business
- interview and front-desk areas where your people are separated from clients and the public
- military bases and airside work areas with a security fence around the perimeter and controlled entry points
- vehicle-based work where the vehicle is fitted with a security container, alarm and immobiliser
- exhibition areas with security controls and controlled public access.

In zone 2, you can:

- store information and physical assets with a BIL up to **very high**

- use information and physical assets with an **extreme** BIL, (but this information should not normally be stored in the area and you must use approved security containers)
- use information and physical assets with a **catastrophic** BIL only under exceptional circumstances to meet operation imperatives with approval of the originating agency. No storage is permitted.

Zone 3 - Restricted work areas

These are security areas with high security controls. They provide access controls to information and physical assets where any loss would result in a business impact up to **extreme**. They also provide protection for people.

Access for your people and contractors is limited to those with a need to access the area. People with ongoing access must hold an appropriate security clearance. Visitors must be escorted, or closely controlled, and have a business need to access the area.

Examples of restricted areas are:

- secure areas within your building that have extra access controls for your people (such as IT server rooms)
- exhibition areas with very valuable assets
- areas with high-value items or items of cultural significance when not on display.

In zone 3, you can:

- store information or physical assets with a BIL up to **extreme**
- use information or physical assets with a **catastrophic** BIL (but the information or assets should not normally be stored in the area).

Zone 4 - Security areas

These are security areas with higher levels of security. They provide access controls to information where any would result in a business impact up to **extreme**, and physical assets where any loss would result in a business impact up to **catastrophic**. They also provide protection for people.

Access for your people is strictly controlled with ID verification and card access. People with ongoing access must hold an appropriate security clearance. Visitors and contractors must be closely controlled and have a business need to access the area.

Examples of security areas are:

- secure areas within your building that have extra access controls for your people
- exhibition areas with very valuable assets with specific item asset protection controls and closely controlled public access
- areas used to store high-value items or items of cultural significance when not on display.

In zone 4, you can:

- store information or physical assets with a BIL up to **extreme**

- use information or physical assets with a **catastrophic** BIL (but the information or physical assets should not normally be stored in the area).

Zone 5 - High-security areas

These are security areas with the highest level of security controls. They provide access controls to information or physical asset where any loss would result in a business impact up to **catastrophic**.

Access for your people is strictly controlled with ID verification and card access. People with ongoing access must hold an appropriate security clearance. Visitors and contractors must be closely controlled and have a business need to access the area.

Examples of high-security areas are:

- areas storing TOP SECRET, sensitive, or compartmented information
- New Zealand Intelligence Community facilities.

In zone 5, you can store information marked TOP SECRET, compartmented information, or large quantities of information that when aggregated have a **catastrophic** BIL.

PSR security zone requirements table

	Level of assurance required for information and physical asset sharing				
Control components	Zone 1	Zone 2	Zone 3	Zone 4	Zone 5
Building construction	Determined by an agency's risk assessment	**During business hours** Normal construction to the New Zealand Building code **Out of hours** Construction to NZSIS *Technical Note – Physical Security of Intruder Resistant Areas*	Construction: • To NZSIS *Technical Note – Physical Security of Secure Areas* for information only, or • Using elements tested to AS 3555.1-2003 level 4 or above for valuable physical assets	Construction: • To NZSIS Technical Note – Physical Security of Secure Areas for information only, or Using elements tested to AS 3555.1-2003 level 4 or above for valuable physical assets	Construction: • To NZSIS Technical Note – Physical Security of Zone 5 Areas
Out of hours Alarm Systems	Determined by an agency's risk assessment	Determined by an agency's risk assessment, recommended for office environments AS/NZS 2201 Class 3-4 alarm which hard wired within the Zone	AS/NZS 2201 Class 4 alarm hard wired within the Zone (use of NZSIS approved detection devices is recommended). Separate from EACS and BMS.	AS/NZS 2202 Class 5 alarm hard wired within the Zone or NZSIS Approved Alarm installed to the approved instructions. Must use NZSIS-approved detection devices.	NZSIS Approved Alarm installed to the approved instructions. Must use NZSIS-approved detection systems
Out of hours Alarm response	Determined by an agency's risk assessment		Determined by an agency's risk assessment. Response should be within the achieved delay from other physical security measures.		

	Level of assurance required for information and physical asset sharing				
Control components	Zone 1	Zone 2	Zone 3	Zone 4	Zone 5
Access control systems	Determined by an agency's risk assessment	Determined by an agency's risk assessment, recommended for office environments ID card required for access. Recommended authentication in.	ID card and sectionalised access control system with authentication in.	ID card and sectionalised access control system with authentication in and out. Full audit trail maintained.	ID card and sectionalised access control system with authentication in and out. Full audit trail maintained.
Locks – after hours mechanical	Determined by an agency's risk assessment	Determined by an agency's risk assessment Agency's buildings should be locked out of hours and for prolonged power failure.	Commercial locking system	NZSIS approved locking system	NZSIS approved locking system
Locks – access controls	Determined by an agency's risk assessment	Commercial locking system	Commercial locking system	NZSIS approved locking system	NZSIS approved locking system
Keying systems for all locks	Determined by an agency's risk assessment	Commercial restricted keying system recommended. Inline key systems not recommended.	NZSIS approved keying system	NZSIS approved keying system	NZSIS approved keying system
Interoperability of alarm system and other building management systems	Determined by an agency's risk assessment	Determined by an agency's risk assessment. IF a SAS and separate EACS are used the SAS cannot be disabled by the access control system.	Separate alarm system which cannot be disarmed by the access control system	No network level communication with other systems. Cannot be controlled by other systems.	No network level communication with other systems. Cannot be controlled by other systems.
Visitor control	Determined by an agency's risk assessment	Visitor register with visitors escorted in sensitive parts of the facility.	Escorted visitors in whole of zone.	Visitors excluded unless there is an identified need.	Visitors excluded unless there is an identified need. Visitors must be escorted.
Storage of official information	Determined by an agency's risk assessment See "Selecting security containers and cabinets"				
Storage of valuable physical assets	Determined by an agency's risk assessment See "Selecting safes and vaults"				
Other controls to address specific risks	Determined by an agency's risk assessment. See "Additional controls to address specific risks."				

Additional Resources

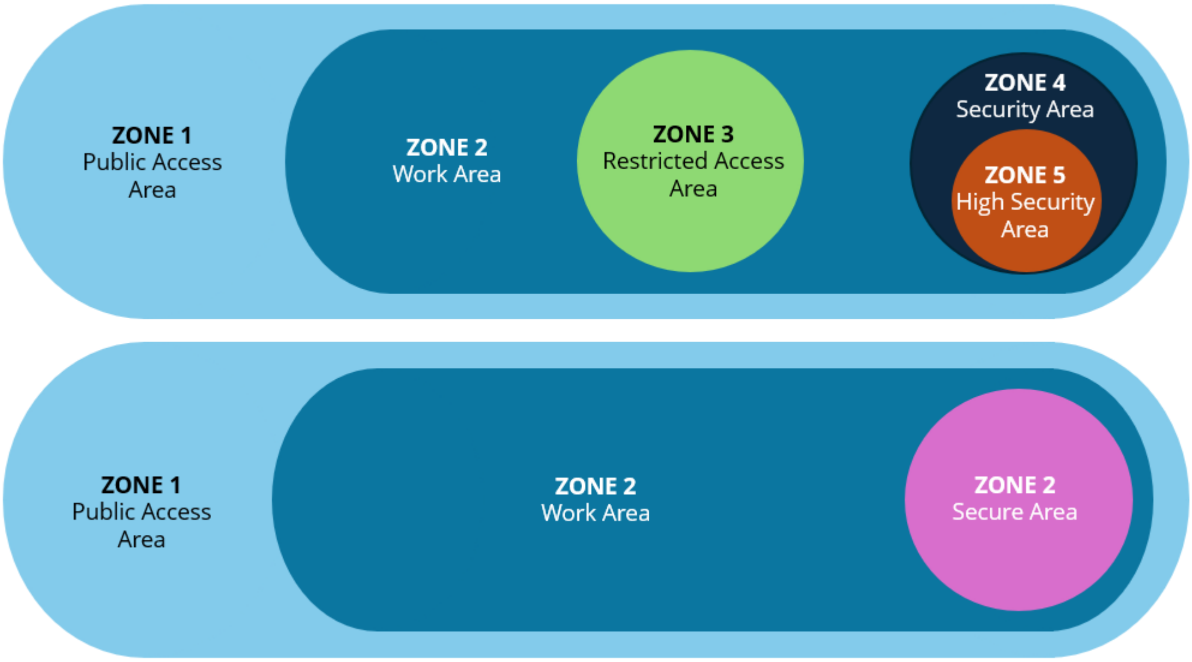
Resource	Purpose
Applying Business Impact Levels	Business impact level matrix and definitions
Physical security measures checklist [DOCX, 37KB]	Checklist to help organisations to determine security zone designation for facilities or areas.
Selecting security containers or rooms for storing official information [PDF, 99KB]	Table describing requirements for selecting storage containers or rooms for each zone
Selecting safes or vaults for protecting valuable physical assets [PDF, 39KB]	Table describing requirements for selecting safes or vaults for each zone
Storage requirements for electronic information in ICT facilities [PDF, 73KB]	Table describing requirements for electronic information in ICT facilities for each zone.

Appendix D: Achieving security in depth

To achieve security in depth, layer the zones, working in from Zone 1 and increasing the protection with each new zone.

The following diagram shows a possible combination of security zones to achieve security in depth.

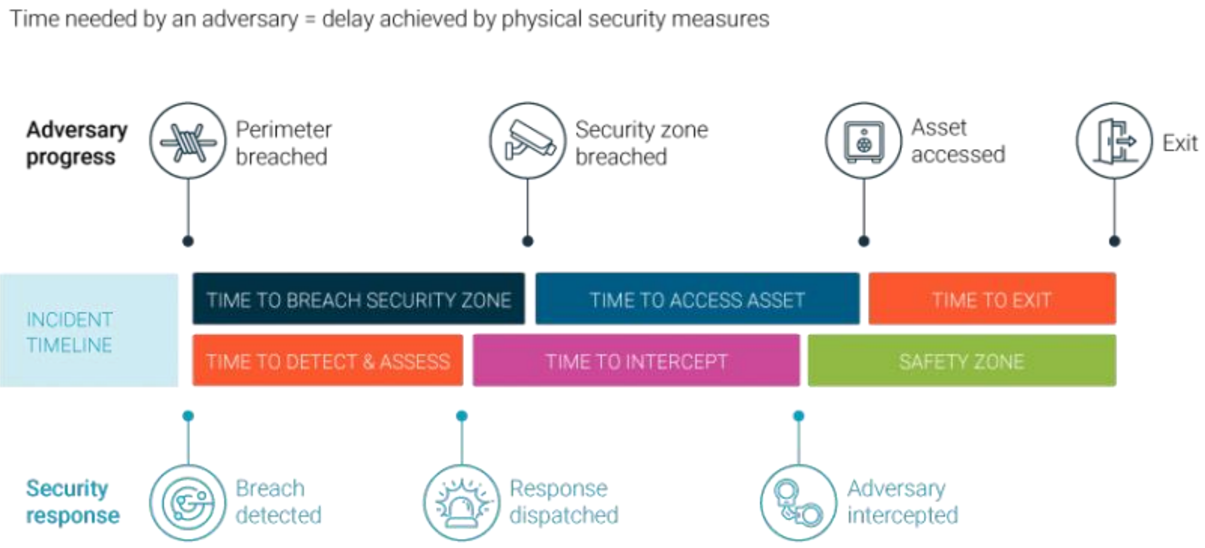
Diagram 1 - Achieving security in depth by layering security zones



Because the security levels increase in line with the zones, you will be creating longer delays with each new layer you add. The cumulative delay gives you more time to respond to any attempts at unauthorised entry to the inner zones.

The following diagram shows how security in depth can provide enough delay for an effective security response.

Diagram 2- Security incident timeline



As the zone levels increase, your protective security measures should progressively change to protect information and physical assets.

The number of zones you need depends on the different levels of assurance and segregation required.

Sometimes, it isn't possible for higher zones to be located fully within lower zones. In those cases, consider strengthening the external walls and security measures for the perimeter of the higher zones.

Zone 1 should include perimeter protection measures. For example, to control visitors, the direction of flow of pedestrians and vehicles, blast mitigation, counter-terrorism protection and so on.

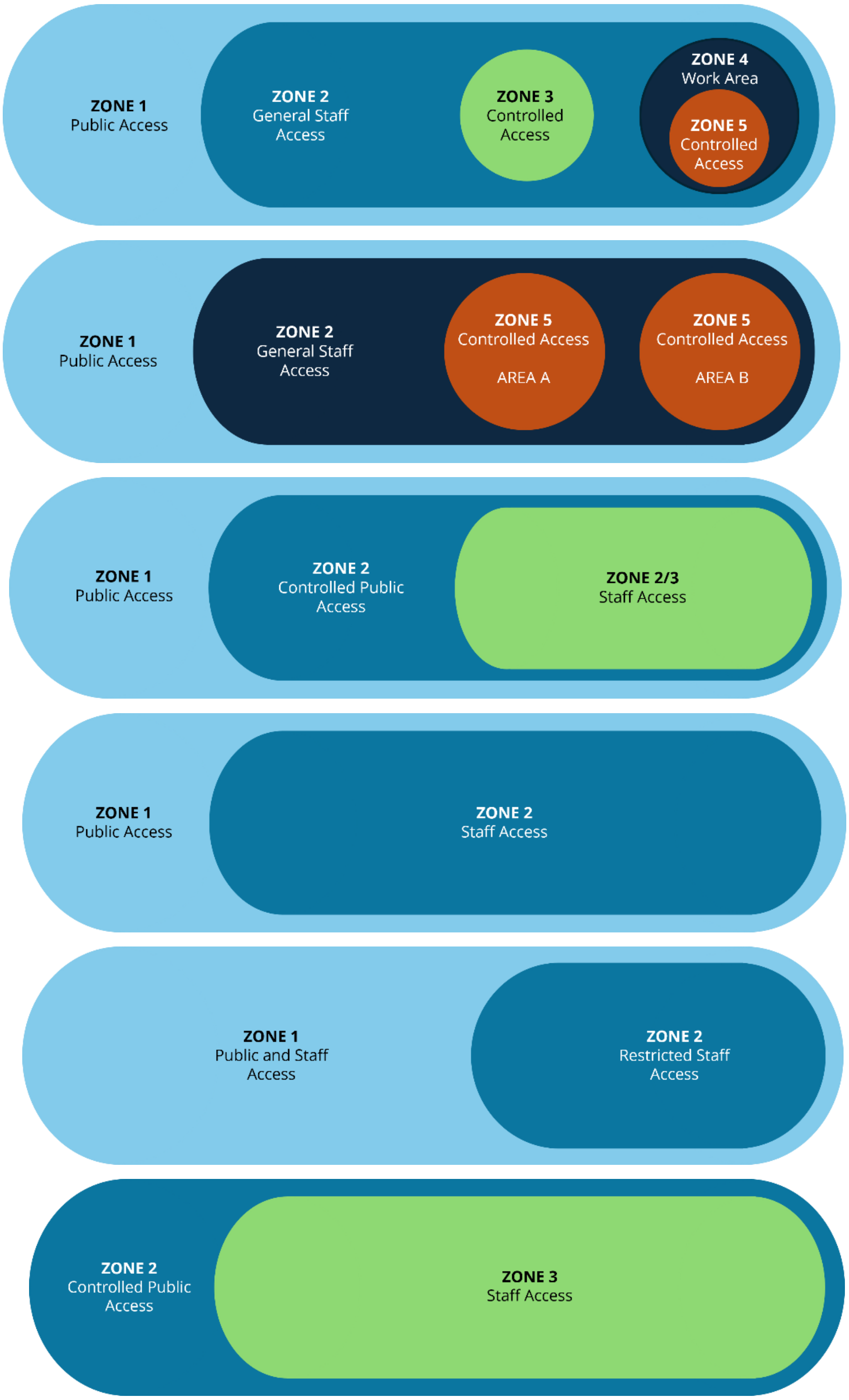
You should work out the minimum and maximum zones required in your facilities. For example, organisations with:

- BILs of low to medium may only need zone 1 or zone 2 unless additional health and safety risks are identified
- BILs up to, and including, high to very high may need zone 1 and zone 2
- BILs up to, and including, extreme will need zones up to and including 3 or 4
- BILs up to, and including, catastrophic will need multiple zones 1 to 5

For more on the BILs, go to Applying the Business Impact Levels.

Diagram 2 shows some of the different ways that you can layer zones to provide increased protection.

Diagram 3 - Combining security zones to increase protection



Appendix E: Good Practice Physical Security Design practices

Deter, Detect, Delay, Respond, Recover

Physical security measures aim to protect people, information, and assets from compromise or harm through the following defensive principles.

Deter

Deter or discourage unauthorised people from attempting to gain unauthorised access to your facility. Implement measures that unauthorised people perceive as too difficult or needing special tools and training to defeat.

Detect

Detect unauthorised access as early as possible. Implement measures to work out whether an unauthorised action is occurring or has occurred.

Delay

Delay an unauthorised access attempt for as long as possible to allow an effective security response to be activated. Implement measures to slow the progress of a harmful event.

Respond

An effective response counters the anticipated activity of an unauthorised person within a time appropriate to the delay measures. Prepare measures to prevent, resist, or mitigate the impact of an attack or event.

Recover

Take the steps required to recover from a security incident. Plan to restore operations to as near normal as possible in a timely manner following an incident.

Crime prevention through environmental design

Crime Prevention Through Environmental Design (CPTED) should be an integral part of your facility planning.

To apply the principles of CPTED, identify which aspects of the physical environment could affect people’s behaviour and then use that knowledge to design an environment which minimises crime.

Always base your security measures on your organisation’s risk assessment, as CPTED alone might not meet all your security needs.

More information on CPTED

Many publications deal with CPTED in the domains of private housing and public areas, but the principles apply equally to government organisations.

National Guidelines for Crime Prevention through Environmental Design

Ministry of Justice, 2005

Designing out Crime: Crime Prevention through Environmental Design

Australian Institute of Criminology, 1989

Crime Prevention through Environmental Design (3rd edition, 2013) by Timothy Crowe M.S. Criminology - Florida State University, revised by Lawrence Fennelly.

Appendix F: Relevant standards for design of physical security measures

When your organisation is implementing physical security measures, use the following standards, handbooks, and codes to guide you.

Standards

Australian and New Zealand Standards (AS and NZS)

AS/NZS 2343:1997 Bullet-resistant panels and elements (under review)

AS/NZS 3016:2002 Electrical installations - Electric security fences (under review)

AS/NZS 2201.5:2008 Intruder alarm systems - Alarm transmission systems

AS/NZS 2201.1:2007 Intruder alarm systems - Client's premises- Design, installation, commissioning and maintenance

AS 2201.3:1991 Intruder alarm systems - Detection devices for internal use

AS 2201.2:2022 Intruder alarm systems - Monitoring centres

AS 4145.2:2008 Locksets and hardware for doors and windows - Mechanical locksets for doors and windows in buildings

AS/NZS ISO 45001:2018 Occupational health and safety management systems - Requirements with guidance for use

AS/NZS IEC 60839-11-1:2019 Electronic access control systems - System components requirements (Part 11-1)

AS/NZS IEC 60839-11-1:2019 Electronic access control systems - Application guidelines (Part 11-2)

AS3555.1-2003 Building Elements – Testing and Rating For Intruder Resistance Intruder-Resistant Panels

AS HB 328:2009 Mailroom Security

British Standards (BS)

BS EN 1143-1:2019 Secure storage units. Requirements, classifications and methods of test for resistance to burglary. Secure safe cabinets

BS 1722–14:2016 Fences – Specification for open mesh steel panel fences

BS 1722–12:2016 Fences – Specification for steel palisade fences

En50131-2-2:2021 Requirements for passive infrared detectors

Din 699 Shredders

International Organization for Standardization (ISO)

ISO 22343-1:2023 Security and resilience – Vehicle security barriers – Part 1: Performance requirement, vehicle impact test method and performance rating

ISO 22343-2:2023 Security and resilience – Vehicle security barriers – Part 2: Application

ISO 31000:2018 Risk management - Guidelines

Japanese Industrial Standard (JIS)

JIS S 1037 – Fire proof safe testing standard

UL Standards

UL 72 – Tests for fire resistance of records protection equipment

UL 687 – Burglary-resistant safes

UL 768 – Combination Locks

UL 634 – Standard for Connectors and Switches for Us with Burglar-Alarm Systems

Handbooks/Guides

New Zealand Government Property Group Guidance and Workplace design

HB 167:2006 Security risk management

HB 327:2010 Communicating and Consulting About Risk

Designing out Crime: Crime Prevention Through Environmental Design

IES-G-1-16 Guideline on Security Lighting for People, Property, and Public Spaces

Privacy and CCTV: A guide to the Privacy Act for businesses, agencies and organisations

New Zealand Information Security Manual (NZISM)

Codes

The New Zealand Building Code

Guidance for constructing PSR security zones

The following protectively-marked material will guide you on the construction and security of PSR Security Zones. Contact the PSR team for more information.

NZSIS Approved Products List (APL)

NZSIS Technical Note – Class A Secure Room

NZSIS Technical Note - Class B Secure Room

NZSIS Technical Note - Class C Secure Room

NZSIS Technical Note – Physical Security of Intruder Resistant Areas

NZSIS Technical Note – Physical Security of Secure Areas

NZSIS Technical Note – Physical Security of Zone 5 Areas

Appendix G: Event Security

Whether an organisation is hosting or attending events, an organisation MUST assess physical security and safety risks and put measures in place to reduce them.

Event organisers have common law duties and statutory obligations under New Zealand legislation to protect people attending events.

Events are many and varied but include New Zealand Government events and overseas events.

Some government events are in the national interest, such as the Waitangi Day and ANZAC Day celebrations.

Before the event

Consider protective security and safety requirements in the earliest stages of event planning.

You have common law duties and statutory obligations under New Zealand legislation to protect people attending events. You may also need to protect information and assets.

To plan an event well, you need to:

- appoint qualified people to security roles
- consider the threats
- develop a security plan
- inspect possible venues
- manage event preparation.

Appoint an event manager and event security officer

The event manager is responsible for overall event security. The manager must appoint an event security officer (ESO) as early as possible, so they can be included in the planning process.

The ESO is responsible for implementing security for the event and the event venue, and should be competent in security management.

Your ESO should:

- be senior enough to exercise the necessary authority
- have direct access to the event manager
- have a sound knowledge of protective security.

For a large or long-running event, the ESO might need a support team.

Common duties of an ESO

The duties of the ESO should include, but are not limited to:

- seeking advice on possible threats to the event
- completing a security risk assessment for the event or venue(s)
- preparing any security plans based on the risk assessment activity

- making necessary security preparations for the event
- coordinating security during the event
- liaising with appropriate people from your organisation, or external agencies and authorities before, during, and after the event.

Consider the possible threats

Considering possible threats to the event and preliminary work on the event plan usually happen at the same time.

The ESO should seek advice on possible threats from:

- the part of your organisation that is coordinating the event and any other relevant parts
- external agencies, such as the New Zealand Security Intelligence Service (NZSIS) and the New Zealand Police when relevant.

You should identify, assess, and manage the risks to an event in line with the principles in:

- ISO 31000:2018 Risk management - Guidelines
- HB 167:2006 Security risk management.

Assessing threats to national security

The ESO should seek a threat assessment from the NZSIS's Combined Threat Assessment Group (CTAG) if:

- the event could be the subject of terrorism or violent protest
- previous similar events have been subject to terrorism or violent protest

If you request for a threat assessment, include enough details on the event to enable CTAG to carry out a robust and thorough assessment.

If you become aware of any additional relevant information after the original threat assessment is issued, advise CTAG and they will publish an updated threat assessment.

CTAG may also issue updated threat assessments if it becomes aware of any relevant information.

Protecting high-level and foreign guests

New Zealand's obligations under the following conventions and legislation may impact on event security:

- Convention on the Prevention and Punishment of Crimes Against Internationally-Protected Persons, including Diplomatic Agents 1973
- Vienna Convention on Diplomatic and Consular Relations
- Crimes (Internationally Protected Persons, United Nations and Associated Personnel and Hostages) Act 1980
- Diplomatic Privileges and Immunities Act 1968
- Consular Privileges and Immunities Act 1971.

When to contact specialist agencies

Department of Internal Affairs

If you're planning a non-routine event that high-level officials will attend, contact The Visits and Ceremonial Office of the Department of Internal Affairs.

Examples of high-level officials are:

- New Zealand holders of high office — for example, the Prime Minister or the Governor-General
- members of the diplomatic or consular corps at ambassador level.

Ministry of Foreign Affairs and Trade

If you're planning an event that high-level foreign dignitaries or controversial visitors who could attract protest activity will attend, contact the Ministry of Foreign Affairs and Trade's Protocol Division.

Email: prd@mfat.govt.nz

Examples of foreign dignitaries are heads of state, heads of government, foreign ministers or other senior level ministers.

Develop an event security plan

Your ESO should develop a security plan based on a risk assessment of the event.

The plan will evolve as details of the event become clearer, and preparations for the event develop. It will also depend on the duration, location, and size of the event.

Remember to include any event security arrangements in the event costings.

If an event will be held overseas, consult with the Ministry of Foreign Affairs and Trade (MFAT) in the early planning stages to work out if the proposed location and venue is suitable. This consultation is particularly important if:

- protectively-marked or commercially sensitive information will be accessed or used at the event
- New Zealand dignitaries will attend the event.

Use the following questions to prompt your thinking and planning. Add any special requirements you have to the plan.

Identify what you need to protect and when

Think about the need to protect the proceedings themselves, any documents (both those provided and notes taken during the event), and people who attend.

What kinds threats are there? What is the appropriate level of security for the event?

How long will the event last? Will the protection needs stay constant throughout the event or vary? When might you need to increase protective measures?

Will attendees be making visits to other sites or activities as part of the event?

Which is the best site for the event?

You might have different sites to choose from — some within your facilities and others at external venues. Questions to answer include:

- How much control do you need to have over the event? (The less control you have, the more likely it is that extra security measures will be needed.)
- How sensitive is the information that will be present? Do you need protection from oversight or overhearing?
- What are the unique risks posed by each site?
- How will the flow of the event affect your choice?
- What are the transport options?
- Will you be able to protect the attendees?
- What will you do if threats to the event materialise?

Inspect possible venues before you decide.

For events where sensitive and protectively-marked information will be present, it's best to choose a venue controlled by a New Zealand Government organisation.

To assess a venue, your ESO should refer to Assess your physical security risks.

Who will be involved in running the event and what are their roles?

How will you manage communication between different parts of your organisation, or with other organisations involved in running the event?

What are the roles and responsibilities of event staff?

Who is responsible for liaising with the New Zealand Police if necessary? For example, if the event might attract protest action.

Who will attend the event?

Who are the attendees? Who do they work for or represent? Will any overseas people attend? Any New Zealand or overseas office holders? Any media representatives or members of the public?

Are there any security clearance or character check requirements for attendees?

Will any VIPs attend and need personal protection?

Do you need to arrange accommodation for VIPs or other attendees? What are their accommodation security requirements?

What are your contingency plans?

Contingency plans might include communications, command and control arrangements, and alternative venues for incidents (for example, bomb alerts and public demonstrations or protests).

How will you protect the event?

Detail the threats you've identified and the measures you plan to use to manage the risks.

Think about any special protective security measures you might need. For example, audio countermeasures, or security containers and other security equipment.

If your event will involve, SECRET, TOP SECRET or codeword/sensitive compartmented information (SCI), - and at a premise accredited for that level of information - your ESO should seek advice from the NZSIS and GCSB based on your risk assessment. Then state in your event plan what measures you will put in place. For example, you might need to:

- strictly limit the number of invitees to the overall event
- strictly limit the number of invitees to particular sessions
- limit the duration of the event to as short a period as practicable
- keep handouts to a minimum
- secure the meeting room from audio-visual recording devices
- plan for handling and storing information before and after each day
- plan for destruction of information that is no longer needed.

If necessary, your chief security officer can seek advice from the Government Communication Security Bureau (GCSB) on technical surveillance counter measures.

Inspect possible venues

Inspect possible venues at the earliest opportunity. Find out what security is already available and what you might have to put in place. Note any potential risks you haven't already identified.

Your ESO should accompany the event organiser during a preliminary inspection or provide advice on security requirements if they can't attend.

If protest activity is a possibility, involve the local police at an early stage of your event planning. A more detailed inspection might be required later, once you've chosen a venue. At both stages contact with local police and venue management can be useful for gaining local knowledge.

When you inspect a venue, consider the following questions.

What might adversely affect physical security?

Would it be easy or hard to fix problems? For example, door locks and window catches, curtain fittings, exterior lights, and light fittings.

Can you control access to the venue?

Include entry to the venue, rooms within the venue, and any onsite parking.

Is there an area where you can examine suspicious articles?

If you needed to detonate an explosive device, it would need to be done in an area where it caused minimal damage to property and no injury to anyone.

How vulnerable is the venue to overhearing, overlooking, and electronic eavesdropping?

Your risk assessment will inform the level of security you need for these aspects.

Once you've selected a venue, a more detailed survey might be needed.

Manage event preparation

Based on your security plan and inspection of the venue, you may need to address several matters before the event.

These include processes, arrangements, security controls, and logistical matters.

You may need processes for:

- controlling keys
- controlling entry
- managing an emergency evacuation
- reporting security incidents
- receiving and escorting visitors
- storing, handling, and disposing of official or protectively-marked information.

You may also need to arrange or prepare:

- event set up schedules
- a communication plan
- event security instructions
- supply and delivery of security containers and other security equipment
- event access and identity passes
- security clearances
- event security exercises
- technical surveillance counter measures
- employees or guards to control access
- searches to sanitise the premises.

During the event

The event security officer oversees security and is responsible for many important tasks during the event.

Responsibilities during the event

As well as overseeing security arrangements at the event, the event security officer (ESO) may have to conduct or oversee many tasks to ensure event security is well managed.

Communication, awareness, and advice

The ESO may need to:

- liaise with the event manager on communications, command, and control issues
- maintain awareness of, and consistency with, health and safety requirements
- provide event attendees and venue employees with security advice, including security and emergency procedures

- advise attendees of the protective marking of the subject matter and the security arrangements and facilities available (the security classification of topics to be discussed should be displayed at the start of the event and again before each protectively-marked segment of the event).

ID and entry control

The ESO may need to:

- ensure accredited attendees are issued access and identity passes, including ensuring identities are verified if necessary
- control entry to ensure that no unauthorised persons gain access to the building or event, or can observe or listen to proceedings
- supervise security aspects of visitor control

Safety of protectively-marked information

The ESO may need to manage arrangements for protectively-marked information used and produced at the event, including how it is received, recorded, distributed, transmitted, returned, and stored. Ensuring its secure storage may include coordinating:

- the use of security containers
- waste collection and disposal.

For more information, see the policy **INFOSEC 2.3.d: Handle government information securely**.

Personnel coordination

The ESO may need to:

- coordinate security procedures for cleaning and maintenance personnel
- coordinate the physical security and storage of equipment (for example, cameras, recording devices, audio-recording devices, and mobile phones)
- supervise people employed on security duties
- supervising any necessary searches to sanitise the premises.

Note: An ESO should seek advice from their organisation's chief security officer when needed to help with investigating any security incidents.

Managing event accreditation

Event accreditation documents provide speedy validation of a person's right to attend an event.

Major events should have:

- a master list of participants, including event management and support staff (where possible, featuring photo identification and information covering roles, contact details, etc)
- accreditation passes for participants, featuring:
  - identity verification

    - photo identification
    - the dates of validity
    - the category of participant
    - any restricted area access rights
- a design and layout that can be visually checked by guards or event staff.

Accreditation passes should be designed so that they are comfortable for participants and can be worn at all times.

When an event is sensitive and you need to avoid publicity, consider using a unique but unobtrusive identification article, such as a lapel pin or badge.

Controlling access to restricted areas

Your ESO should decide which event areas need to have restricted access — areas within the venue to which only certain attendees, authorised officials, and security staff will have unescorted access.

Clearly label restricted access areas and control access to them.

Managing information security

Information used at an event could be in a variety of forms, including the proceedings themselves, documents brought to or produced at the event, and audio-visual presentations.

Protectively-marked information

Based on the event risk assessment, the ESO should consider not allowing attendees to bring any protectively-marked information.

If protectively marked information is needed at the event, consider the following protective measures:

- distributing the necessary number of copies at the beginning of the event, or if possible, at the session where they'll be needed
- increasing accountability by numbering and recording the distribution of each copy
- arranging for attendees to leave all protectively-marked documents, including any notes taken, at the end of the session or day, and send the documents by safehand to each delegate after the event.

Whether these measures are practical will depend on the circumstances of the event.

Whatever arrangements are made, the ESO should inform attendees of them as early as possible and, if necessary, remind attendees during the event.

Protectively-marked waste

If protectively-marked waste will be generated at the venue, the ESO is responsible for ensuring there are adequate facilities to collect and dispose of it.

For some protectively-marked information, you might need to use an approved shredder or removal/destruction procedure at the venue.

Also refer to the policy **INFOSEC 2.3.d: Handle government information securely**.

Security containers

At times, it may be necessary to store protectively-marked information onsite either during the event or between proceedings if the event runs for more than one day.

In this case, the ESO may need to ensure suitable security containers are provided and will be responsible for controlling access to them.

For help with using the right security containers, go to **Physical Security Appendix J: Specific security measures** subsection **Security containers and cabinets**.

Using technical security

You must use technical surveillance countermeasures (TSCM):

- before and during an event that involves TOP SECRET, SECRET, or SCI/codeword information
- when the security plan or threat assessment indicates the need for them.

Your ESO should contact the Government Communications Security Bureau (GCSB) for advice before any event that is TOP SECRET.

The ESO should also seek advice from the GCSB if information and communications technology (ICT) equipment will be required for processing protectively-marked information.

Considering guards and guard patrols

Your event risk assessment should tell you whether you need guards and guard patrols during an event.

If an event runs for longer than one day, your ESO should consider regular guard patrols during hours the venue is not attended.

If you need to carry out a TSCM sweep to sanitise the premises, you should consider guarding to minimise the risk of a post-sweep compromise.

Reporting security incidents

Advise event attendees to report any security incident to your ESO or security staff straight away, so the situation can be dealt with swiftly.

Security staff should report any incidents to the ESO as soon as practical after becoming aware of the incident.

The ESO should refer to **GOV 6: Manage security incidents**.

Issuing security and emergency instructions

Everyone who will be attending or working at the event needs to know what your security and emergency instructions are. However, you might need separate instructions for staff and participants.

Your ESO should issue the security and emergency instructions for attendees at the event either they arrive or on arrival.

Receiving mail

Make sure you've considered the necessary requirements for receiving mail or goods that may be delivered to an event, including procedures for scanning and handling suspicious items.

Controlling demonstrations

The New Zealand Police have ultimate responsibility for controlling demonstrations.

If your event security risk assessment indicates that demonstrators may be a problem, seek advice from the police at an early stage to ensure they can respond or are available to discuss other mitigation strategies, including the deployment of security guards.

Your ESO is responsible for ensuring proper arrangements are in place before the event begins.

Handling media attention

Media attention might be focused on the event. This attention could be because of event publicity, attendance by VIPs, or the subject matter.

Developing a media plan

If you're organising the event, consult your ESO when you're developing your media plan. The plan may include, based on the risk assessment:

- accreditation of, and passes for, media representatives
- a designated room at the venue for media representatives
- procedures for issuing media releases and statements
- a requirement that, on arrival, media representatives report to the event security or reception area.

Make sure you:

- consider carefully whether any media representative is to be permitted into the venue or event rooms at any time while the event is in progress, and if so, under what conditions
- ensure any release to the media is in line with your organisation's media liaison processes
- ensure any media access is under controlled conditions and with appropriate escort arrangements
- ensure you take particular care to prevent unescorted access to any room where protectively-marked information could be left unattended (prevent access until the room has been checked for protectively marked information).

After the event

Your event security officer carries out tasks that ensure the event is wrapped up securely.

Post-event responsibilities

Following the event, the event security officer (ESO) completes the following tasks when necessary:

Retrieving or disabling access and identity passes

If event access and identity passes give unescorted access to your organisation's venue, the ESO coordinates retrieving all passes. If that is not possible, the ESO must disable any access provided by the passes.

Searching the venue

The ESO coordinates a thorough search of the venue to ensure no official information or assets that belong to your organisation have been left behind.

For example, items such as documents, audio-visual recordings, whiteboards, projection equipment, and electronic media equipment.

Returning security containers (if used)

The ESO coordinates the return of any security containers used at the event, including changing combination settings for container travel and storage.

Submitting a security report

The ESO submits a security report to the event organiser.

Reporting any unreported security incident

For any security incidents that occurred during the event that have not already been reported, the ESO reports in line with **GOV 6: Manage security incidents**

Returning protectively-marked material

The ESO arranges the secure transmission of any protectively-marked event papers and documentation to all attendees.

Appendix H: Physical security for ICT systems

Introduction to physical security for ICT systems

ICT systems are protected by a combination of physical and logical controls. Logical access controls are detailed in the New Zealand Information Security Manual.

Make sure you refer to security requirements for ICT systems and electronic information in your organisation's business continuity plans, and other disaster response and recovery plans.

You may need to consult the GCSB before you install ICT systems.

Exceptions come with conditions

If your organisation must apply the logical controls identified in the New Zealand Information Security Manual, and must meet or exceed (based on your risk assessment) the controls identified in the PHYSEC 2.

You should also:

- ensure your chief security officer (CSO) is involved in planning processes for ICT systems, so that the physical security requirements are suitable for the ICT equipment and operations
- restrict access to ICT equipment used to store or process official information to authorised people with a need-to-know
- provide physical security to all components of your ICT systems, including cabling, taking into account the highest level of classification of any system.

More guidance:

For more guidance on ICT system security, refer to the following documents.

- NZS/AS ISO/IEC 27002:2022 Information technology – Security techniques – Code of practice for information security management
- ANSI/TIA-942 Telecommunications Infrastructure Standard for Data Centers

Outsourced ICT facilities

Meet your obligations to protect information when you outsource ICT facilities.

Your organisation must ensure that outsourced ICT facilities meet the physical security requirements for ICT systems.

Preparing to use a data centre

Before you use a data centre, you must assess the aggregated (combined) value of the official information you plan to store in it. Information can increase in value when it is combined and therefore need greater protection.

If you have a shared data centre arrangement, work with the other organisations to assess the Business Impact Level (BIL) of the aggregated information before you use the datacentre operationally.

Protect data storage devices in line with the business impact of the compromise of the aggregated of the information stored on the devices.

Data centres can provide security for your information and ensure your information is continuously available.

ANSI/TIA-942 Telecommunications Infrastructure Standard for Data Centers

Using a commercial data centre

If your organisation plans to use a commercial data centre to hold official information with BIL of catastrophic, you must seek advice from the New Zealand Security Intelligence Service (NZSIS). They will advise you on the certification requirements for the physical security measures that you must meet before the data centre is used.

GOV 5: Manage Risks when working with others guides you on including security requirements in contracts for outsourced functions.

Secure your ICT equipment

Physical security measures for ICT equipment help to ensure your organisation stays operational.

ICT equipment is essential for processing, storing, and communicating your organisation's information.

Which ICT equipment you need to protect

ICT equipment that requires protection includes any device that can store information electronically, such as:

- computers — desktop, laptop, or tablet
- photocopiers, multi-function devices (MFDs), and printers
- mobile phones
- digital cameras
- personal electronic devices
- storage media — for example, portable hard drives, USB sticks, CDs, DVDs, radio frequency identification (RFID) tags and systems
- network equipment — for example, routers, switches
- voice systems — for example, PABX.

Where to locate ICT equipment

You should locate ICT equipment in a security zone that is suitable for protecting either the aggregate of information stored on the equipment, or the value of the equipment, whichever requires the greater protection.

How much protection to give ICT equipment

Base the level of protection you give to ICT equipment on the highest Business Impact Level (BIL) that would result from:

- the compromise, loss of integrity or unavailability of the aggregate of electronic information held on the equipment, or
- the loss or unavailability of the ICT equipment itself.

Using tamper-evident seals

You can seal access to ICT equipment using New Zealand Security Intelligence Service (NZSIS) approved tamper-evident wafer seals suitable for application to hard surfaces.

Seals may give a visual indication of unauthorised access into the equipment if the seals are removed or broken.

Refer to the Approved Products List (APL) when selecting wafer seals. This list is protectively-marked, contact the PSR for more information.

Where to store ICT equipment when not in use

When your ICT equipment is stored in dedicated ICT facilities, meet the physical security controls detailed in the supporting documents below.

When your ICT equipment is not stored in dedicated ICT facilities, apply the physical security controls in Security zones.

Add any additional controls when you need to based on your security risk assessment.

If your organisation can't meet the requirements, seek advice from the Government Communications Security Bureau (GCSB) on additional logical or technological solutions that may be available to lower the risks to electronic information when your equipment is not in use.

When ICT equipment can't be kept in security containers or rooms

You may not be able to secure some electronic equipment in security containers or rooms when not in use. For example, desktop computers, printers, and MFDs.

To find an appropriate solution, first assess the BIL of the equipment and the information it holds.

Remember that the logical access controls described in the New Zealand Information Security Manual don't constitute sanitisation and reclassification of ICT media. Therefore, the media retains its protective marking for the purposes of reuse, reclassification, declassification, sanitisation, destruction and disposal as specified.

If the following information doesn't solve your problem, seek advice from the GSCB on additional logical or technological solutions that may be available to lower the risks to electronic information.

Non-volatile media, such as hard drives

In some circumstances, you may be able to fit removable non-volatile media (such as hard drives) that can then be secured in an appropriate security container when not in use.

If the non-volatile media can't be removed, work out which zone the equipment can be kept in based on the risk of unauthorised people obtaining information and the sensitivity of the information held in the equipment.

Equipment with solid state drives or hybrid hard drives

Solid state drives and hybrid hard drives can't be made safe through normal wiping processes when switched off.

If you wish to use equipment fitted with solid state drives or hybrid hard drives, seek advice from the GCSB on other methods for securing these types of equipment (for example, encryption).

Information or equipment with BILs of very high, extreme, or catastrophic

If the BIL of the equipment and/or information it holds is very high or extreme, the equipment should be stored in a zone 3 or above area.

If the BIL is catastrophic, the equipment should be stored in a zone 5 area, unless you are able to apply additional logical controls to lower the risks to a level acceptable to the originator.

How to deal with removing ICT equipment from your premises

Your organisation must have a policy on removing ICT equipment from your facilities that prohibits your people from doing so without permission.

New Zealand Information Security Manual - Working Off-Site and Working Away from the Office has more information.

Keeping ICT equipment secure when it's offsite

You must apply physical security measures to off-site equipment that address the risks to the equipment and the information it holds. Apply the logical controls detailed in the New Zealand Information Security Manual - Distributed Working.

How to audit your ICT equipment

For asset control of ICT equipment, record the location and authorised custodian, and audit periodically.

The period between audits should be based on your risk assessment, with higher risk items audited more regularly.

If your risk assessment suggests it is warranted, consider visually inspecting your ICT equipment as part of your asset control audit to ensure non-approved devices have not been installed.

You should have processes that your people can use to report the loss of ICT equipment.

Secure your ICT system equipment

Protect your information lifelines.

Which ICT system equipment needs physical security

As well as the ICT equipment mentioned in Secure your ICT equipment, you need to have physical security in place for:

- servers, including dedicated devices and laptops used as servers
- other communication network devices — for example, PABX

- supporting network infrastructure — for example, cabling and patch panels
- gateway devices — for example, routers, and network access devices.

Where to locate servers and network devices

Servers and network devices must be located in security rooms, or in containers that are in security rooms and protected in line with their Business Impact Level (BIL).

It's best to keep servers and communication network devices in dedicated ICT facilities. If any of your servers and network devices not held in dedicated ICT facilities, apply the controls identified in **Physical Security Appendix C: PSR Security Zone Requirements**.

For more information, refer to:

- New Zealand Information Security Manual (NZISM).
- **GOV 5: Manage Risks when working with others**

Protecting network infrastructure

Your organisation can lose control of their information when it is communicated over an unsecured public network infrastructure or over infrastructure in unsecured areas.

Protect network infrastructure using a mixture of physical security measures and encryption.

If you apply GCSB-approved encryption, the physical security requirements can be lowered.

You must use security zones suitable for the highest BIL of the information being communicated over the network infrastructure.

As it may not be possible to secure all network infrastructure in security containers or rooms, you should also meet any system encryption requirements in the NZISM.

Protecting ICT system equipment with containers

Work out the level of container required for patch panels, fibre distribution panels, and structured wiring enclosures based on:

- the business impact of the information passing over the connections
- any other controls in place to protect the information.

Panels should, at a minimum, be in locked containers and/or rooms to prevent tampering.

Applying encryption standards

When the BIL of the information transmitted over public network infrastructure is high or above, your organisation must use the encryption standards identified in the NZISM.

The encryption will give enough protection to allow the information to be transmitted on an unclassified network.

In unsecured areas, you must apply the encryption standards identified in the NZISM to protect information on your network infrastructure.

Keeping cabling secure

To keep cabling secure, apply the cabling security controls in the NZISM – Infrastructure.

Cabling must be kept in a Zone suitable for the use of the level of information carried.

Maintaining equipment

To ensure the availability and integrity of your information, maintain equipment in line with the manufacturer's directions.

Protecting deployable ICT systems

It can be difficult to apply suitable physical security measures when you use deployable ICT systems, particularly if they're deployed into high-risk environments.

You should seek advice from the GCSB or Department of Internal Affairs (DIA) on suitable logical controls to help mitigate any risks you identify.

DIA should be consulted for items classified as restricted or below. GCSB should be consulted for items classified as CONFIDENTIAL and above.

Protecting ICT system gateway devices

In addition to the logical controls required in the NZISM, you must use physical security measures for your ICT system gateway devices to mitigate the higher business impact from:

- the loss of the devices
- the compromise of the aggregated information arising from physical access to the devices.

If you're using shared gateways, you must apply controls to the gateway appropriate to the highest level of information passing through the gateway.

You must prevent unauthorised access to gateway devices. It's best to locate these devices in dedicated ICT facilities.

Protecting equipment from power disruptions

Protect ICT equipment from power failures and other disruptions. Aim to achieve an uninterrupted power supply to ICT systems, particularly servers, so your organisation can continue operating. If that's not achievable, aim for enough power to at least close down systems.

Prepare for disasters

Protect ICT systems and equipment from disasters.

Including ICT in your business continuity plans

Your organisation's disaster recovery and business continuity plans should include availability requirements for information held in ICT equipment.

The impact of the information not being available will influence the measures you take to protect ICT equipment against environmental and human threats.

For more information, refer to section 4.7 of HB 292-2006: A Practitioner's Guide to Business Continuity Management.

Preserving ICT equipment

ICT equipment may require a controlled atmosphere to:

- ensure the integrity of the information held within it
- prevent failure of the equipment and potential loss of information.

Controlling the atmosphere may include controlling:

- temperature
- humidity
- air quality — for example, smoke and dust
- water

Make sure you meet the requirements identified by the manufacturer when you apply atmosphere controls.

Advice on preserving electronic information for the future is available online from Archives New Zealand.

Using uninterruptible and auxiliary power supplies

If your ICT systems are unexpectedly shutdown, you may lose information. An uninterruptible power supply (UPS) may allow you to turn off systems in a controlled manner or provide power until power to your ICT system is restored.

Any UPS you use should provide at least enough power to allow:

- the controlled shutdown of ICT systems
- the start-up of an auxiliary power supply.

ICT equipment also needs protection from power surges (relatively lengthy increases in voltage), and power sags and spikes (short, very large increases in voltage). Most UPSs also give some protection from surges and sags.

As most environmental systems rely on mains electricity, an auxiliary power supply may help you maintain environmental controls.

Auxiliary power supplies should be maintained in line with the manufacturer's directions.

Assessing risks from disasters

Your organisation should identify any environmental or human-induced threats humans to their ICT equipment in their security risk assessment.

As ICT systems may be more sensitive to environmental factors, you may need extra risk mitigation measures, over and above those used to protect people and physical assets from harm.

Protecting against flooding

Water is one of the major threats to any system that uses electricity, including ICT systems.

Site server rooms should be protected against flooding. Flooding may be from external sources (for example, swollen rivers) or internal sources (for example, burst pipes).

If you’re considering locating any server rooms in basements, assess the risk of flooding from internal or external sources.

Protecting against fire

ICT equipment can be damaged through direct exposure to flames, from the effects of smoke (poor air quality), and increases in temperature in the general environment.

Another concern is the potential for flooding during fire-fighting operations. You may be able to use alternatives to water-based sprinkler systems, such as CO_2, or other gaseous agents in critical ICT facilities. Base your decision to use alternatives on your risk assessment.

Using back-up ICT systems

Back-up ICT systems can provide a recovery point if your primary ICT systems fail. Back-up systems can form part of your business continuity and disaster recovery plans.

Any back-up system should be, as far as possible, fully independent of the supporting infrastructure used for the primary system so that if the primary ICT system fails, the back-up system does not also fail.

Back-up ICT systems should be regularly tested to ensure their continued operation.

You may use off-site or commercial back-up facilities. Consider dual redundancy. That is, using two back-up facilities for business-critical information and ICT systems.

Ensure that any commercial ICT facilities you use meet all the mandatory security requirements for protecting New Zealand Government information.

If you use a commercial back-up facility, consider the aggregation of information held in the facility, not just your own information, when you work out the levels of physical and logical security needed at the facility.

Information on including security requirements in contracts for outsourced functions is available in **GOV 5: Manage risks when working with others**.

Secure your ICT facilities

Protect your ICT facilities and the information held within them.

ICT facilities

Your organisation should have dedicated ICT facilities to house your ICT systems, components of your ICT systems, or ICT equipment. These facilities might include, but are not limited to:

- server and gateway rooms
- data centres
- back-up repositories
- storage areas for ICT equipment that hold official information
- communications and patch rooms.

Pay particular attention to the security of any access points to an ICT facility. For example, cabling and ducting.

Accreditation of ICT facilities

Your ICT facilities must be:

- within accredited security zones
- appropriate for the value of the aggregated (combined) information held within them
- in security zones dedicated to these ICT facilities and separate to other functions.

When you outsource your ICT facilities or use shared facilities, you must ensure your information is held in a security zone appropriate to the value of the aggregated information.

Securing containers used to house ICT equipment

Containers used to house ICT equipment in an ICT facility may be at a lower level when the ICT facility is in a separate security zone within an existing security zone that is suitable for the aggregation of the information held.

Storage requirements for electronic information in ICT facilities tells you more.

Securing ICT facilities for information with TOP SECRET or compartmented markings

ICT facilities that hold information with TOP SECRET or compartmented markings must be in a separate zone 5 that is within a zone 5 work area, both of which must be certified by the New Zealand Security Intelligence Service (NZSIS).

Controlling access to ICT facilities and equipment

Your organisation must control access to ICT facilities in line with **Physical Security Appendix C: PSR Security Zone Requirements.**

Access to ICT facilities holding information with a Business Impact Level (BIL) lower than catastrophic should be controlled by:

- a dedicated section of the SAS or EACS, where used
- a person provided with a list of people with a 'need-to-know' or need to go into the ICT facility.

Your organisation must keep ICT facilities secured when they are not occupied, including security containers within the facilities that hold ICT equipment.

When people need security clearances

Anyone who can access your ICT servers, work in areas that contain ICT servers, or work in areas where your ICT assets are stored must have a national security clearance. The level of security clearance depends on the BIL of the aggregated information, but a CONFIDENTIAL clearance would be required as a minimum.

Refer to the Guide to personnel security for your organisation.

Your organisation should supervise access to ICT servers, restricting access to a need-to-know basis.

Using technical surveillance countermeasures (TSCM)

If you have an ICT facility that holds information with TOP SECRET and compartmented markings and regular discussions at a TOP SECRET level are held within it, a technical surveillance countermeasures (TSCM) inspection is required.

A TSCM inspection may also be required to provide a high level of assurance that hardware and cabling infrastructure within an ICT facility has not been compromised.

When your organisation doesn’t require its ICT facilities to handle TOP SECRET information, base the requirement for a TSCM inspection and the interval between inspections on your risk assessment.

Refer to the Using technical surveillance countermeasures and audio security in Other physical security measures.

For more advice on TCSM inspections, contact the **GCSB**.

Appendix I: Securely transporting sensitive items

To protect sensitive items, follow the four stages of secure transportation.

The tasks for securely transporting sensitive items fall into four broad stages:

- assessing the risks
- planning security before you move the item
- managing security during the move
- confirming the item has arrived safely and wrapping up the transport process.

1. Assessing the risks

Sensitive items can be transported in several ways. For example, when people in your organisation:

- carry items with them (by hand or in a bag)
- work remotely or abroad (for example, from home or a hotel)
- transport items in a vehicle.

Understand the threats you need to manage

Whichever way an item is transported, many potential threats exist. For example, an item could be:

- accidentally lost or damaged
- accident on route
- stolen by an opportunistic thief
- abandoned because of an emergency
- taken from a hijacked or stolen vehicle
- attacked by someone inside your organisation
- targeted through espionage.

Carry out a risk assessment

Use a risk assessment to help you understand:

- the value of the item you need to transport
- the business impact on your organisation if the item was lost or damaged
- the likely threats to the item during transport.

Based on your assessment, consider which security measures will achieve the best balance between robust security and operational effectiveness.

2. Planning security for the item

To plan effectively, answer the following questions.

What is the nature of the item?

Describe the item's size, purpose, value, and any significant features that might affect how it is transported.

If the item has a security classification with associated security requirements, ensure you include those requirements in your plan.

Who is involved?

Identify everyone involved in the transport process and what they are responsible for.

Will the process involve getting sign-off from a manager, liaising with a courier, or arranging an escort? Who will receive the item when it's delivered?

How and when will the item be moved?

Describe how and when the item will be moved.

What mode of transport will be used? Which routes will be involved? Are there any waypoints to consider? What is the destination?

When is the move happening? Does the intended date and time pose any risks? Consider things like traffic volumes, predicted weather, and major events.

What are the likely risks to the item?

Based on your risk assessment, consider risks from the local environment and the planned route.

What is security like at the sites the item is moving from and to? What is the terrain like on the planned route? Is traffic a concern? Will border security be involved?

Which security measures will best protect the item?

Detail the security measures you'll use. Ensure the measures are proportionate to the risks you identified in your assessment; and enable everyone involved to effectively manage the transport process.

What are your contingency plans?

If the item is compromised, how will you respond to and manage the situation? Do you have alternative transport plans?

Does everyone involved know what to do?

Make sure you provide the right training and task-specific briefings to the relevant people. They must know how to protect the item and what to do if anything goes wrong.

3. Managing the item's security during travel

Keep the following practices in mind when you're managing security while items are being moved.

Maintain awareness

Scan your surroundings and be alert to potential threats, especially when escorting others.

Keep a low profile

Be discreet. This practice includes the people involved being discreet and the equipment you use to protect an item being discreet.

Communicate as planned

Be prepared to provide status updates as planned or to call for assistance when you need to.

Check your physical security solutions

Ensure security solutions are working as intended. For example, solutions designed to mitigate threats such as opportunist theft, forced entry, or covert attempts to gain unauthorised access.

4. Confirming the item’s safe arrival and wrapping up the process

Once an item has been transported, you need to:

- check the item has arrived intact and hasn’t been compromised
- confirm its delivery with the recipient or owner (for example, with a receipt)

You also need to:

- assess the entire procedure to find out if it was carried out without issues en route
- record details of the transfer for auditing purposes.

Best practice guidelines for transporting sensitive items

Follow these guidelines to keep sensitive items secure when they’re being transported.

Terms and definitions used in these guidelines

- **Sensitive item:** Any item which, if compromised, would have an adverse impact on the owner; or any individual, organisation, or nation connected to the item.
- **Owner:** The organisation, individual, or author to whom the sensitive item belongs.
- **Custodian:** An organisation or individual that the owner entrusts with sensitive items by the owner to act on behalf of the owner.
- **Authorised person:** A trusted individual granted unaccompanied access to sensitive items by the owner in accordance with the needs of their job.
- **Transport container:** A holding container in which sensitive items are transported between the owner’s site and an external storage or destruction facility.

Choosing the right containers

When you transport sensitive items, they must be in containers that are discreet, opaque, locked, and strong.

Each container must be fitted with a tamper-evident seal and fixed or locked to the vehicle’s chassis before transportation.

If you transport sensitive and non-sensitive items in the same vehicle, they must be in separate containers.

In a closed-bodied or box vehicle, you can use a load compartment that is not accessible from the driver’s cab as a transport container.

You can't use an open-bodied or curtain-sided vehicle as a transport container, but you can use it to carry containers.

Securing vehicles before and during use

Fit

Before you use a vehicle to transport sensitive items, depending on your assessment of risk, it should be fitted with:

- an audible anti-theft alarm and immobiliser, which must be armed when the vehicle is unattended
- a remote tracking device that makes the location of the vehicle available to the owner.

Lock

You should keep the vehicle cab locked, except when allowing the driver or passengers to enter or exit the vehicle.

Attend

The vehicle must be attended by one or two authorised persons dependant on the risk assessment and logistical considerations (i.e. rest stops).

Communicate

Vehicle crew or pedestrian couriers should have a communication device they can use safely and legally while in motion to communicate with the owner, the receiver of the sensitive items (for example, an external destruction facility), and emergency services.

Planning and altering routes

Your custodian must have a documented route plan for the vehicle, including any planned stops and business continuity procedures, which must be agreed in advance with the owner.

Your custodian must record any deviations from the planned route and inform the owner before or on arrival at the destination.

Stopping while transporting sensitive items

A vehicle transporting sensitive items can stop at a location other than the owner's site or external destruction facility. However, the vehicle must:

- not stop for longer than necessary
- have an authorised person in the vehicle while stopped, or the items in the physical control of an authorised person.

Inspect

At the end of each stop, the crew must visually inspect the exterior of the vehicle for signs that someone has accessed or attempted to access the vehicle or transport containers. If signs are detected, the crew must immediately notify the owner or custodian and seek their guidance on what action to take.

Collecting sensitive items from multiple sites

When sensitive items in multiple sites belong to one owner: In a single journey, you can use a vehicle to collect sensitive items from multiple sites if they belong to one owner. However, you can't unload anything from the vehicle until it reaches the destruction facility, and you can't use the vehicle to transport items between the owner's sites.

When sensitive items in multiple sites belong to different owners: In a single journey, you can't use a vehicle to transport sensitive items that belong to different owners.

Delivering sensitive items to multiple destruction facilities

In a single journey, you can use a vehicle to deliver sensitive items to multiple destruction facilities. However, you can't use the vehicle to:

- collect anything from a destruction facility
- transport items between destruction facilities.

At each external destruction facility, your inventory of unloaded items must be verified before the vehicle departs.

Loading and unloading sensitive items securely

You must load and unload sensitive items within a secure perimeter when possible. When it's not possible to establish a secure perimeter, each person who loads or unloads the sensitive items must be escorted by at least one authorised person who is not carrying anything.

During loading and unloading the vehicle you use must also be attended and observed by at least one authorised person.

Following business continuity processes

Keeping driver hours within health and safety requirements

Your custodian must have a documented process for ensuring that drivers don't go over the health and safety requirements for driving hours. The plan should also aim to minimise unplanned stops due to drivers exceeding the driving hours limit.

If the anticipated driving time to a destination would result in all planned drivers exceeding the health and safety requirements, the vehicle must not depart from the owner's site carrying sensitive items.

When unforeseen circumstances mean that all planned drivers have reached driving hour limits, you must follow your crew replacement process (see below).

Worktime and logbooks - nzta.govt.nz

Replacing a crew

Your custodian must have a documented process for minimising unplanned stops due to unforeseen circumstances relating to the crew — unforeseen circumstances such as fatigue, illness, injury, or having exceeded the legal limit for driving hours.

When unforeseen circumstances mean the crew can't continue transporting sensitive items, a replacement crew must be available to complete the journey.

Both crews must follow the requirements in Stopping while transporting sensitive items.

The owner must be notified of the replacement crew and the reason for it as soon as possible.

Replacing a vehicle

Your custodian must have a documented process that minimises unplanned stops due to unanticipated circumstances related to the vehicle — unanticipated circumstances such as mechanical failure or an accident.

When a vehicle is no longer able to deliver sensitive items, a replacement vehicle must be available.

An authorised person must secure the sensitive items as soon as possible.

The sensitive items must be:

- supervised when unloaded and loaded into the replacement vehicle by an authorised person
- transported to a secure location agreed with the owner where an inventory must occur.

The owner must be notified of the vehicle replacement and the reason as soon as practicable.

Appendix J: Specific security measures

The following guidance describes the use of specific security measures.

Remember that physical security is a combination of physical and procedural measures. You should develop policies that support your physical security measures and control their use.

Perimeter security controls

Restricting access to your facilities with perimeter access controls can help your organisation to reduce threats.

Some types of perimeter security controls are:

- pedestrian barriers
- vehicle barriers.

Work out if your organisation needs perimeter security controls during your security risk assessment and before you complete any site selection process.

Pedestrian barriers

Pedestrian barriers are used to restrict access through fences or walls by controlling the entry and exit points.

Examples of pedestrian barriers are:

- fences and walls
- locked gates
- gates connected to electronic access control systems (EACS) or alarm systems
- guard stations.

Vehicle barriers

Vehicle barriers are used to prevent hostile vehicle attacks, prevent damage, and protect pedestrian safety. Vehicle related threats range from vandalism to sophisticated or aggressive attacks by determined criminals or terrorists.

Examples of vehicle barriers are:

- gates
- retractable barriers or bollards
- fences and walls
- bunds and berms.

Related standards

ISO 22343-1:2023 Security and resilience – Vehicle security barriers – Part 1: Performance requirement, vehicle impact test method, and performance rating.

ISO 22343-2:2023 Security and resilience – Vehicle security barriers – Part 2: Application

NPSA Hostile vehicle mitigation

Fences and walls

Fences and walls are used to define and secure the perimeter of a facility.

Fences might not be practical in urban environments, particularly in central business districts.

The level of protection a fence gives depends on its:

- height, construction, material, and access control method
- any additional features used to increase its effectiveness, such as toppers, lighting, or connection to an alarm or CCTV system.

If you choose to use fences or walls to deter unauthorised access, you must develop supporting procedures for:

- monitoring and maintaining the fences or walls
- monitoring the grounds for unauthorised access.

Make sure access points provide equivalent security as the barriers provide.

Related standards

BS 1722–14:2016 Fences – Specification for open mesh steel panel fences

BS 1722–12:2016 Fences – Specification for steel palisade fences

AS 1725:2010 Chain-link fabric security fencing and fates

AS/NZS 3016 Electrical installations- Electric security fences

Building construction

Before your organisation leases or constructs any premises, assess the construction methods and materials to find out if they will give the protection you need.

Increasing the level of building security afterwards may be expensive or impossible.

Domestic versus commercial building construction

Typically, buildings are constructed to the New Zealand Building Code. Some older buildings may not meet this code.

Domestic construction provides little protection from unauthorised access. Intrusion for theft is the most common type of unauthorised access. Skilled covert access is normally very hard to detect in domestic situations.

Standard commercial offices may provide more perimeter protection than domestic buildings. However, internal walls, false ceilings, and other common building techniques reduce your ability to protect information and physical assets.

Most commercial office spaces are only suitable for protecting assets and information with a Business Impact Level (BIL) of medium or below.

For sites operating withing a BIL of HIGH or above, the Technical Notes for security zones 2 to 5 must be applied, which will then provide the minimum construction and security components that must be employed.

Adding extra protection with building hardening

If your risk assessment identifies unacceptable risks, you need to add additional elements to address specific risks.

Some examples are:

- lighting
- additional physical barriers or security zones
- forcible attack and ballistic resistance
- blast mitigation measures
- road and public access paths
- hostile vehicle mitigation
- elements of “Designing out Crime: Crime Prevention Through Environmental Design”.

Related standards

AS 3555.1:2003 Building Elements - Testing and rating for intruder resistance - Intruder-resistant panels. This standard provides guidance on very high-grade intruder resistance, such as for high-security vaults.

Using slab-to-slab construction

Slab-to-slab construction prevents access through false ceilings. The walls are joined directly to the floor and to the bottom of the next floor or the roof structure.

Using tamper evident construction and finishes

Complete the wall surfaces to a smooth, clean, light-coloured finish such that any attempt at compromise should be highlighted.

Where you must use slab-to-slab construction

Your organisation must use slab-to-slab construction at the perimeter of security zones, including all access points.

For details on slab-to-slab construction methods, see the NZSIS Technical Note - Physical Security of Intruder Resistant Areas. This note is protectively marked.

Structural changes can affect the integrity of buildings, so seek structural engineering advice before you implement slab-to-slab construction.

When you can go without slab-to-slab construction (with care)

Your access points for zone 1 and zone 2 may vary between business hours and after hours. For example, from internal points (such as controlled office entry points) during business hours to the perimeter of the building or premise after hours (such as the main door).

You can build access points for zone 2 that are used during business hours without slab-to-slab construction providing that the out-of-hours access point has slab-to-slab construction.

Alternatively, you can install an intruder-resistant layer in the ceiling, such as steel mesh, to address the problem of removable false ceiling panels when you need intrusion delays for specific rooms. Guidance on tamper evident barrier construction can be found in the NZSIS Technical Note – Security Grilles.

Be aware that these measures, such as mesh barriers, don't give any protection from over-hearing, so you must not use them where you need speech security.

You should also use tamper-evident building techniques on all perimeter walls to provide indication of attempted unauthorised access.

Constructing zone 3 and zone 4 perimeters

For information on constructing zone 3 and zone 4 areas to store or discuss protectively-marked information or aggregations of information with a Business Impact Level (BIL) of very high damage, refer to NZSIS Technical Note - Physical Security of Secure Areas.

As this technical note is a protectively-marked document, contact the PSR team for more information.

Constructing zone 5 perimeters

For information on constructing zone 5 areas to store TOP SECRET information or aggregations of information with a Business Impact Level (BIL) of catastrophic damage, refer to NZSIS Technical Note - Physical Security of Zone 5 Areas.

As this technical note is a protectively-marked document, contact the PSR team for more information.

Alarm systems

Alarm systems can provide early warning of unauthorised access to your facilities.

An alarm system can be used alongside other measures designed to detect an intrusion attempt, delay an intruder's progress, and give you time to respond. Your alarm systems must be monitored and linked to a predetermined response.

Type of alarm systems

Alarm systems can be broadly divided into two types:

- a perimeter (or external) intrusion detection system (PIDS) or alarm
- an internal security alarm system (SAS).

Alarm systems may be single sector or sectionalised to give coverage to specific areas of risk. Sectionalised alarm systems allow greater flexibility because highly sensitive areas can remain secured when not in use and other parts of the facility are open.

A PIDS can be valuable for organisations with facilities enclosed in a perimeter fence because it will give early warning of unauthorised breaches.

Your organisation should seek specialist advice when designing and installing PIDS.

Managing alarm systems

You must develop procedures for using, managing, monitoring, and responding to an alarm system.

Any contractors employed to maintain a SAS should be cleared to a level appropriate to the information to which they could reasonably be expected to have incidental access.

Use a suitably qualified designer or installer to design and commission any commercial alarm systems.

Make sure each different security zone is a separate alarm section (area) or have a separate alarm system for each zone.

Infrequently accessed areas (e.g., root spaces, inspection hatches, and under-floor cavities) should be monitored at all times.

Related standards

AS/NZS 2201.1:2007 Intruder alarm systems - Client's premises - Design, installation, commissioning and maintenance

AS/NZS 2201.5:2008 Intruder alarm systems - Alarm transmission systems

Managing alarm systems in zone 1 and 2

In zones 1 and 2, you should manage your alarm systems directly but you can outsource operational functions, such as monitoring and maintenance.

You can use guard patrols instead of an alarm system outside of usual work hours. For more information, go to Visitor Control (Out-of-hours guarding).

Managing alarm systems in zone 3 and above

For alarm systems in zone 3 and above, your organisation must have:

- direct management and control
- appropriately cleared (see PERSEC4) and trained staff as privileged operators and users.

In zone 3, you may use guard patrols instead of an alarm system outside of usual work hours. For more information, go to Visitor Control (Out-of-hours guarding).

Keeping personal identification numbers (PINs) secure

Your organisation should ensure all personal identification numbers (PINs) for arming and disarming alarm systems are:

- uniquely identifiable to an individual
- not recorded by the individual
- regularly changed in line with your risk assessment.

Your people must advise your chief security officer (CSO) straight away if they suspect any PINs have been compromised. Your CSO must disable the PIN and investigate any potential security breach.

For more information, go to Reporting incidents and conducting security investigations.

Dealing with engineering/installer codes securely

You must remove the default/engineering/installer user codes from alarm systems at commissioning.

For zones 3 and above, the engineering/installer codes must only be known to appropriately cleared personnel who have access to the zone and authorised to have the privileged access.

When you need to give the code to others for maintenance purposes, you must change the codes as soon as the maintenance work is finished.

Your organisation should develop appropriate testing and maintenance procedures to ensure your alarm system is continually operational.

Choosing a security alarm system (SAS)

Security alarm systems are used to protect information and assets. To choose the right SAS, consider the:

- level of the zone you need to protect
- complexity of the zone's layout
- security level of the information or assets you need to protect.

Also refer to **Physical Security Appendix C: PSR Security Zone Requirements**.

Understanding SAS classes

Five classes of SASs are defined in AS/NZS 2201.1:2007 Intruder alarm systems - Client's premises - Design, installation, commissioning and maintenance. You must only use alarm systems that comply with this standard.

The five classes and their uses are:

- **Class 1 and 2:** base-level systems only suitable for domestic use.
- **Class 3:** mid-level systems suitable for protecting normal business operations in most organisations.
- **Class 4**: mid-level systems suitable for protecting normal business operations in most organisations when used with detection devices and other controls, suitable for protecting information and physical assets in a Zone 3.
- **Class 5**: high security commercial alarm system suitable for protecting information and physical assets with a BIL lower than catastrophic.

Complying with SAS requirements for security zones

When an NZSIS-approved SAS is not mandatory, your organisation should determine:

- whether a commercial SAS is required at your facilities, including any temporary sites, as part of your risk mitigation strategies
- the specifications for any such system
- whether alternative security methods, such as guard patrols, are required as part of your risk mitigation strategies.

Consider whether you need guard patrols as well as an SAS to satisfactorily mitigate your risks.

Zone 2

If you use a commercial SAS in zone 2 it must meet or better the following standard: AS/NZS 2201.1:2007 Intruder alarm systems - Client's premises - Design, installation, commissioning and maintenance Class 3

Also refer to NZSIS security product guides.

Zone 3

A SAS used in zone 3 must be separate from all other systems including access control and building management systems.

If you use a commercial SAS in zone 3 it must meet or better the following standard: AS/NZS 2201.1:2007 Intruder alarm systems - Client's premises - Design, installation, commissioning and maintenance Class 4

Any detection devices should be approved by the NZSIS, refer to the NZSIS Approved Products List.

Zone 4

A SAS used in zone 4 **must** meet the following standard. AS/NZS 2201.1:2007 Intruder alarm systems Client's premises - Part 1: Design, installation, commissioning and maintenance Class 5 or be an NZSIS-approved SAS.

A SAS used in zone 4 **must** be separate from all other systems including access control and building management systems.

Any detection devices used with the SAS **must** be approved by the NZSIS.

Also refer to NZSIS Approval Products List.

Zone 5

NZSIS-approve alarm systems **must** be used for zone 5.

Any detection devices used with the SAS **must** be approved by the NZSIS.

Individual alarm options

Individual alarms can protect people and vehicles from harm.

In some situations, building alarm systems or other facility-wide measures might not give all the protection your people and assets need. For example, when you need to protect:

- people working away from the office
- areas with a high potential for personal violence
- valuable physical assets in public areas
- valuable assets stored in vehicles used for work purposes.

Several individual alarm options are available to supplement your security measures, including:

- duress alarms (fixed, hidden, and mobile options)
- individual item alarms or alarm circuits

- vehicle alarms.

Duress alarms

Duress alarms enable your people to call for help in response to a threatening incident.

To get fewer false alarms, choose duress alarms that are activated by dual-action buttons (users need to press two separate buttons to trigger the alarm).

Fixed and hidden duress alarms

Fixed duress alarms are individual alarms that are monitored remotely. They're normally hardwired and fixed to a location.

Consider equipping your public contact areas with duress alarms if your organisation's risk assessment has identified a potential problem. Public contact areas include reception areas, counters, and interview rooms.

Hidden duress alarms should:

- enable your people to raise an alarm discreetly
- be augmented by procedures that provide an appropriate response.

Relevant standards

AS/NZS 2201.1:2007 Intruder alarm systems Client's premises - Part 1: Design, installation, commissioning and maintenance | Building CodeHub is the standard you must comply with when you configure duress alarms as part of an intruder alarm system. The same standard governs where the alarm panel is located within the protection zones of the alarm system.

Training your people

You need to ensure that your people are aware of any duress alarms, have regular training, and participate in trials so they know what to do in a real situation.

Mobile or individual duress alarms

Mobile or individual duress alarms help to deter violence towards your people. They're suitable for times when your people are outside the office or circulating in public areas.

Personal duress alarms fall into two broad categories:

- alarms that monitored remotely
- alarms that produce loud noise when activated.

Alarms that are monitored remotely

These alarms are suitable for use within facilities where there is a dedicated monitoring and response force. The alarms consist of a personal alarm transmitter linked to the facility or a separate alarm system.

Noise producing alarms

These alarms rely on the response of bystanders. They are more suitable than monitored duress alarms when there could be considerable delay in response to the alarm.

You can use noise-producing alarms within your facility when you need people in the immediate area to notice an incident as soon as it happens.

Individual item alarms and alarm circuits

When you can't easily protect valuable items using normal alarm systems (particularly when they're are in public areas, such as exhibitions) two options to consider are:

- installing a separate alarm system to monitor individual items
- installing an individual item alarm circuit.

Some alarm sensor types that may be suitable are:

- pressure switches
- motion sensors
- closed-circuit television (CCTV) activated alarms
- radio frequency identification (RFID) tag systems.

Seek specialist advice when you're designing alarm systems for individual items.

Vehicle alarms

Consider installing vehicle alarms if your people need to work from vehicles and those vehicles contain large quantities of valuable equipment.

Noise producing alarms

Most vehicle alarms rely on noise to deter intruders. However, if the vehicle driver is outside hearing range, these kinds or alarms rely on a response from bystanders.

Remote alarms

When the Business Impact Level of the information or assets in the vehicle, or the vehicle itself, is high or above, consider fitting vehicle alarms that are monitored remotely.

Remote vehicle alarms can also be linked to remote vehicle tracking and immobilisation systems.

Access control systems

Use access control systems to prevent unauthorised access.

An access control system is a measure or group of measures designed to:

- allow authorised personnel, vehicles, and equipment to pass through protective barriers
- prevent unauthorised access.

Achieving access control

Access control can be achieved in several ways. The most common ways are:

- using psychological or symbolic barriers –e.g., paths, fences, barriers
- positioning security staff to monitor and control access
- installing mechanical locking devices operated by keys or codes
- using electronic access control systems (EACS).

Validating identity using authentication factors

Access control systems should provide identity validation using authentication factors about:

- what you have — keys, identity (ID) cards, and passes
- what you know — personal identification numbers (PINs)
- who you are — visual recognition, biometrics, and so on.

Using EACS

Your organisation must use EACS when there are no other suitable identity verification and access control measures in place.

EACS can be used along with other personnel and vehicle access control measures.

Get expert help

Your organisation should:

- seek specialist advice before selecting EACS
- use a designer or installer recommended by the manufacturer to design and commission EACS.

Follow good practice

Your organisation must verify the identity of every potential cardholder before you issue them with access cards for your EACS.

You must also audit regularly to check who has access to your EACS system. You need to find out who still needs access, and disable or remove access for people who no longer need it or have left your organisation.

You can use sectionalised EACS to control access to specific areas in your facility.

EACS should typically start at zone 2 perimeters, but may be used in zone 1 (for example, to control access to car parking).

Keep your EACS software and hardware up to date. Ensure your software is updated to address known vulnerabilities. Consider updating EACS cards and readers as they age and become vulnerable to new threats.

Relevant standards

AS/NZS IEC 60839-11-1:2019 Electronic access control systems – System components requirements (Part 11-1)

AS/NZS IEC 60839-11-2:2019 Electronic access control systems – Application guidelines (Part 11-2)

Meet the highest threat and risk level

When you implement EACS to cover a whole facility (on their own or with other access control measures), design them to meet the highest perceived threat and risk level.

If you use EACS along with other access control measures, design each system to meet the highest perceived threat and risk level in the areas covered by the system.

Using anti-passback controls in high security areas

When you use anti-passback controls, cardholders can't pass their cards to another person to use and tailgaters can't get through. This control system is valuable for preventing unauthorised access to highly secure environments.

Using a two-person access system to protect highly valuable information and physical assets

Some EACS can be enabled to only allow access to areas when two people are present and can activate an alarm if one leaves the area. This feature is known as a 'no-lone-zone'. It requires two authorised people to access and exit a designated area.

Consider using a two-person access system when you need to protect very highly or extremely valuable information and physical assets.

Implementing an identity card system

Identity (ID) cards allow you to quickly recognise people who work for your organisation.

You must use ID cards in all facilities with security zones 3 to 5.

You should issue ID cards to all people who have regular access to your facilities and meet your personnel security requirements.

Establish high-quality processes first

To build an ID system of high integrity, you need robust processes for verifying identities, and for registering, enrolling, issuing, and auditing ID cards. Consider conducting a privacy impact assessment.

Verify all identities

Before you issue an ID card, you must verify the person's identity. See PERSEC 1 for more information.

Make sure the ID cardholder provides government issued credentials with a photo

Verify security clearance holders

When an ID card will grant access to areas requiring a security clearance, or indicate that the holder has a security clearance, you must independently verify the details of their clearance (including when it expires or is due for revalidation) before you issue an ID card.

Follow good practice

Your ID cards should:

- be worn and clearly displayed at all times in your premises
- be uniquely identifiable
- include a return address for lost cards
- not identify the facility to which the card gives access
- not be worn outside your premises
- be audited regularly in line with your risk assessment.

Remember to protect your:

- card making equipment
- spare, blank, or returned cards.

You can include other information on ID cards to improve your control of access, such as names, photographs, and colours.

Using EACS access cards as ID card is not recommended, particularly in high security or high-risk areas.

Alarm system and other building management systems interoperability

Interoperable systems must be designed carefully to avoid creating vulnerabilities.

Implementing interoperability between security alarm systems (SASs) and other building management systems can increase the threat of unauthorised system access and penetration.

Examples of other building management systems or external integrated systems (EISs) are:

- building management systems (BMSs)
- closed-circuit television (CCTV)
- electronic access control systems (EACS).

When you interconnect systems, ensure your SAS cannot be controlled or disabled by any of your interconnected systems.

Your IT security team should review the implementation of any interconnection.

Interoperability in security zones 1 and 2

SASs suitable for Zone 1 and Zone 2 applications may include fully integrated EACSs as a single system. However, this increases the risk of exploitation by others.

Interoperability in security zones 3 and above

For zone 3 and higher, your SAS and EISs must be separate and independent from each other. Any interoperability must not allow the SAS to be controlled or disarmed by the EIS.

For Zone 4 and 5, no network level communication is allowed with other systems. SAS must not be controllable by other systems.

Interoperability with EISs

Designers of EIS or sub-systems need to secure the EIS to prevent unauthorised access or manipulation, especially when it is interconnected with an SAS. EISs should be designed with appropriate logical and physical controls.

Locks, key systems, and doors

Choose the right hardware to protect your information and assets.

Your organisation must secure all access points to your premises, including doors and operable windows, using commercial grade or NZSIS-approved locks and hardware. These locks may be electronic, combination, or keyed.

You must give combinations, keys, and electronic tokens the same level of protection as the most valuable information or physical asset contained by the lock.

You must use NZSIS-approved locks and hardware in security zones 4 and 5 (refer to NZSIS Guidelines on equipment selection and the Approval Products List).

Use suitable commercial locks or NZSIS approved locks in other areas.

Locks

Locks can deter or delay unauthorised access to information and physical assets.

However, locks are only as strong as the fittings and hardware surrounding them. So assess the level of protection you need from doors and frames when you're selecting locks.

Combination lock settings

Your chief security office (CSO) should manage the security of your lock combinations.

Your people must memorise lock combination settings, and make sure you keep only one written record of each setting for use in an emergency.

Keep the record of the combination in an appropriately sealed envelope and protect it in a container. Protectively mark the envelope with the highest security classification of the material protected by the lock.

Follow the lock manufacturer's instructions when you use or service combination locks.

When to change settings

You must change lock combination:

- when you first receive a container
- after a lock is serviced
- after a change of custodian or other person who knows the combination
- when there is reason to believe the setting has been, or may have been, compromised
- at least every 6 months
- when a container is disposed of by resetting the lock to the manufacturer's settings

When to report a security breach

Your people must immediately report the compromise or suspected compromise of a combination setting to your CSO. For more information, go to Reporting incidents and conducting security investigations.

Using keying systems

If you use a keying system, design it to prevent unauthorised people from making duplicate keys or using common techniques to compromise it.

Keying systems should include security measures. For example:

- legal controls, such as registered designs and patents
- physical controls that make it difficult for people to get or manufacture blank keys or the machinery used to cut duplicate keys

- controls that protect against techniques like picking, bumping, impressioning, and decoding.

Choosing a keying system

When you're choosing a keying system, consider the following questions.

- What level of protection does the system provide against common forms of compromise?
- Is an NZSIS approved keying system required?
- What is the length of legal protection the manufacturer offers?
- What level of protection can the supplier provide for your keying data within their facility?
- How transferable is the system and are there any associated costs?
- What are the costs for commissioning and on-going maintenance?

Complying with security zone requirements

In zone 1, it is recommended that you use restricted keying systems.

In zone 2, you must use restricted keying systems.

In zones 3 to 5, you must use NZSIS-approved keying systems. If your risk assessment shows it's necessary, use approved systems in other zones too.

For more information, go to the NZSIS Guidelines on equipment selection and the Approval Products List.

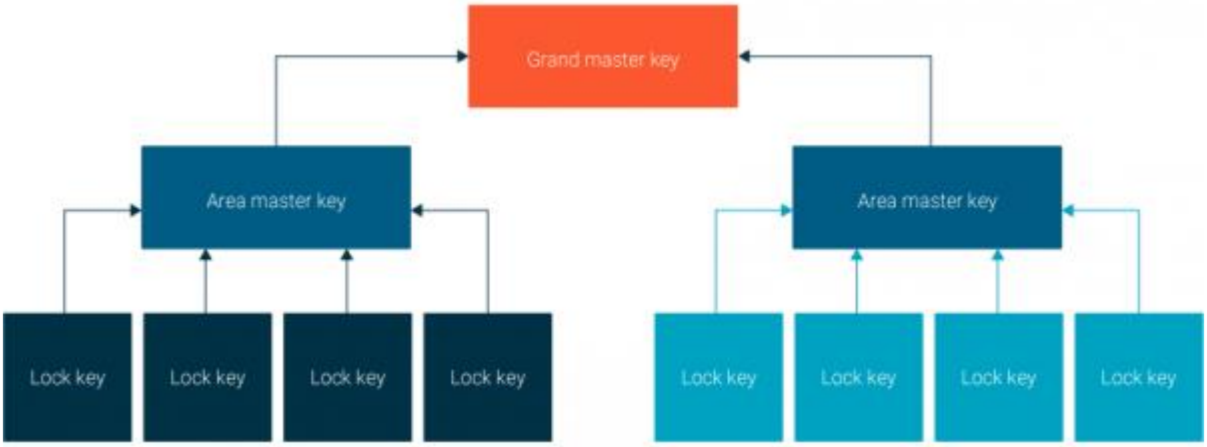
Using mastered key systems

Keys to zones 3 to 5 must not be master keyed.

If you use a mastered key system, it must have enough levels to allow you to have separate area master keys to control any:

- locks within an electronic access control system (EACS)
- alarm system control points.

The following image outlines how mastered key systems allow you to separate and protect different areas.



Managing your keys

You must maintain a register of all keys that you hold and issue. Ensure your key register is secure and only allow authorised employees to access it.

Your key register should include the following details:

- key number
- name, position, and location of person holding the key
- date and time issued
- date and time returned or reported lost

Only people with access to the area to which the key grants access should have access to the key.

Keeping master keys secure

Strictly control your master keys and limit the number of them.

Because master keys may give access to all areas of a facility, your CSO should control the issuing of them.

Audit your key register regularly to confirm the location of all keys. Losing a master key may mean you need to re-key all locks under that master.

Removing master keys from your facilities

Keys to security zones 4 and 5 should not be removed from your facilities.

Keys to security containers must not leave your facilities, except in cases of emergency.

For zones 1 to 3, base any decisions about allowing keys to be removed from your facilities on your risk assessment. Removing keys significantly increases the risk of loss.

When you allow a key to be removed, make sure:

- a manager approves the removal

- you increase the frequency of your key audits

Master keys should not be removed from your facilities.

Ensure everyone in your organisation knows and follows your key management policy.

Protecting your key cabinets

Locate key cabinets within your facility's secure perimeter and, where possible, within the perimeter of the zone where your locks are located.

Key cabinets may be either manual or electronic.

Many commercial grade key cabinets provide very little protection from forced or covert access.

NZSIS approved Class C keys and keys to Zones 3 to 5 must be stored in:

- NZSIS-approved key safe
- NZSIS-approved Class B or C security container

Access to key cabinets should be limited to persons authorised to access all keys contained within the cabinet. Access or visibility of keys can facilitate compromise.

Electronic key cabinets

Electronic key cabinets may have an automatic audit capacity and supplement the need to maintain a key register.

In some cases, electronic key cabinets can be integrated into an EACS. Most commercial grade electronic key cabinets are not suitable for high security applications. Guidance on selecting electronic key cabinets can be found in the NZSIS Security Product Guide - Electronic Key Cabinets. This guidance is protectively-marked. Contact the PSR team for more information.

Electronic key cabinets protecting keys in Zone 3 areas and above, or Class C security containers, must be listed in the NZSIS Approved Products List (APL). The information in the list is protectively marked. Contact the PSR team for more information.

Doors

Select doors that provide a similar level of protection to the locks and hardware you've fitted.

Incorporate any requirements of the **New Zealand Building Code** and any disability access requirements.

Door types and requirements for Zone 2 are specified in the NZSIS Technical Note – Physical Security of intruder resistant areas. Door types and requirements for Zones 3 to 4 are specified in the NZSIS Technical Note - Physical Security of Secure Areas. Door types and requirements for Zone 5 are specified in the NZSIS Technical Note - Physical Security of Zone 5 areas. Both these notes are protectively marked. Contact the PSR team for more information.

Types of doors

There is significant variation in commercial office door types. These include, but are not limited to:

- solid core timber

- composite timber
- metal framed insert panel
- metal clad solid core or hollow core
- glass swing opening
- rotating glass
- glass sliding: single and double.

Solid core wood or metal clad doors typically provide the most robust security where they have glass or grill insert panels. The panels and fixings must provide the same level of protection as the door.

Automatic sliding glass doors normally operate through an electric motor and guide fitted to the top of the door. Some of these doors, particularly when unframed, may be levered open either at the centre joint for double sliding doors or sides for double and single sliding doors. This can make them difficult to secure without fitting drop bolts, lower guides, and/or door jambs.

Domestic hollow core doors and **domestic sliding glass doors** provide negligible delay as they are easily forced. However, if you fit them with appropriate locks, they'll give some evidence of an intrusion when broken.

Door Frames

Aluminium frames can commonly be easily spread and provide little or no resistance to forced entry.

Timber frames provide limited resistance to forced entry

Closed-circuit television

Consider using CCTV when your organisation is developing 'security in depth' for a site.

CCTV is a visual deterrent to unauthorised access, theft, or violence. It can be used to cover:

- site access points, including internal access to higher security zones
- site perimeters
- access to specific physical assets or work areas.

CCTV also gives a visual record of access for audit purposes.

Considering CCTV

The benefits of CCTV may include being able to:

- monitor event-activated alarms
- use it along with a security alarm system (SAS) to help those responsible for responding to the alarm
- use it along with an access control system to aid personal identification for remote site entry control
- use motion detection

- use visual analytics (suspicious package detection)
- Aid investigation into security events.

However, a CCTV system can be a significant capital cost. On-going monitoring, maintenance, and support costs may also be high.

You will also have to comply with all relevant jurisdictional legislation governing CCTV usage. For information about complying with the Privacy Act 2020, refer to the Privacy Commission's guide: **What are my Privacy Obligations Regarding CCTV in New Zealand?**.

Other considerations on the use of CCTV include:

- how its use fits into your overall security plan for the site
- which types of security incidents you anticipate and what your expected response to those incidents might be
- how you will advise your people and visitors that it is in use on the premises
- what your functional requirements are.

If you will use CCTV to support criminal proceedings, the quality of images or data should be suitable for use as evidence.

Be aware that:

- computers used to store CCTV images may require significant memory space.
- excessive compression of data may severely affect the quality of images stored.

You should also consider how long you will need to retain the images.

Seek specialist advice before you design and install a CCTV system to ensure the proposed system meets your needs.

Security lighting

Using lighting to enhance physical security at your site.

Lighting can make an important contribution to physical security. It can be used inside and outside your facility to reduce risks and increase safety.

When you're designing a site, consider what you need to achieve with your security lighting. For example, you might need to:

- deter unauthorised entry
- deter unwanted behaviour when used with other CPTED principles like line of sight
- help guards conduct patrols
- illuminate areas with CCTV coverage
- provide employees with safety lighting in car parks.

Motion detection devices can also be set up, so any detected movement activates lighting or CCTV (or both). Make sure any lighting you use meets the illumination requirements of any CCTV systems you have installed.

- IES-G-1-16 Guideline on security lighting for People, Property and Public spaces

- National Guidelines for Crime Prevention through Environmental Design Ministry of Justice, 2005
- Designing out Crime: Crime Prevention through Environmental Design Australian Institute of Criminology

Security containers and cabinets

Choose the right containers and cabinets to keep information and assets secure.

You must secure official information, valuable physical assets, and money in containers that are appropriate to their Business Impact Level (BIL).

Evaluate your security needs first

When you're selecting security containers and cabinets, evaluate the potential risks to the information or assets they will hold. Risks such as theft, damage, or unauthorised access. Consider the issue of multiple users and/or oversight of information collectively being stored.

Factors that will affect the class of security container you need include:

- the level of protective marking on information or assets
- the BIL
- the location of the information or physical assets within a facility (refer to **Physical Security Appendix C: PSR Security Zone Requirements**)
- the structure and location of your building
- your access control systems
- other physical protection systems you use (for example: locks, alarms, and outer zone security) which make up your total security in depth.

Choosing secure containers

- Table - Selecting security containers or rooms for storing official information this table.

Carefully consider where to put containers

Whenever possible, avoid placing security containers against security zone perimeters with lower levels of protection. Doing so could allow an intruder to bypass the additional security features of the more secure zone.

Consider the weight of the container and floor loading limits.

Protect in line with the highest BIL

Ensure valuable physical assets that contain official information, such as computers and other ICT equipment, are protected from whichever has the higher BIL:

- the compromise of aggregated information in the physical asset
- the loss of the physical asset itself.

When possible, store protectively-marked information separately from other physical assets. This separation will:

- lower the likelihood of information being compromised if physical assets are stolen

- help investigators determine the reason for any incidents involving unauthorised access.

Using NZSIS-approved containers

NZSIS-approved security containers are designed for storing protectively-marked information. Use an approved container when the level of protectively-marked material requires it.

NZSIS-approved security containers provide:

- a high level of tamper evidence from a covert attack
- a significant delay in the event of a clandestine attack
- limited protection from a forcible attack.

Container classes

NZSIS-approved containers come in three classes according to the level of protection they give.

NZSIS-approved containers may not be appropriate for protection of assets and valuable items.

Class A containers

These containers are designed to protect information with a BIL of extreme or catastrophic in high-risk situations.

Class A containers are extremely heavy and may not be suitable for use in buildings with limited floor loadings.

Class B containers

These containers are designed to protect information with a BIL of:

- extreme or catastrophic in low-risk situations
- high or very high in higher risk situations.

Class B containers are broadly of two types:

- heavy types suitable for use where there are minimal other physical controls
- lighter models designed for use along with other physical security measures.

Consider where you will position Class A and B containers, as weight may be an issue, particularly in older buildings.

Class C containers

These containers are designed to protect information with a BIL:

- up to extreme BIL in low-risk situations and information
- of medium in higher risk situations.

These containers must be fitted with an NZSIS-approved restricted keyed lock or padlock.

Consider where you will position Class C containers, as weight may be an issue, particularly in older buildings.

When you don't need an NZSIS-approved container

Your organisation should, where your risk assessments indicate, use lockable commercial containers for:

- information with a low-to-medium business impact
- higher level information – see this table.

Secure rooms, safes, and vaults

Consider using a secure rooms, safes, or vaults instead of containers to protect large quantities of official information or valuable physical assets.

More information

- Safe and vault types
- Selecting safes or vaults for protecting valuable physical assets

Choosing safes and vaults

Store unclassified material in commercial safes and vaults designed to give a level of protection against forced entry that matches the BIL of the assets.

Commercial grade security safes and vaults provide varying degrees of protection, so seek the advice of a qualified locksmith or manufacturer. They'll tell you which criteria you need to use when you're choosing a commercial safe or vault.

Safes and vaults can be fire-resistant (either document or data), burglary-resistant, or a combination of both.

Seek advice from a reputable manufacturer before you install a commercial safe or vault for protecting valuable physical assets.

For items that you can't secure in safes or vaults (such as large items), use other controls that give the same level of intrusion resistance and delay. Use this table.

Fitting vehicle safes

Consider fitting vehicle safes to vehicles used to carry valuable physical assets or official information.

Vehicle safes provide some protection against opportunistic theft. However, they're not designed to protect vehicles left unattended for prolonged periods (for example, overnight).

Vehicles safes are of similar construction to low-grade commercial security containers.

Your risk assessment may show that you need additional controls to mitigate some risks when vehicles are used to transport protectively-marked material or valuable assets.

To ensure the effectiveness of a vehicle safe, consider:

- bolting the safe to the vehicle (preferably out of sight)
- fitting anti-theft controls such as immobilisers and alarms.

Following best practice: NZ and international standards

The New Zealand Standard AS/NZS 3809:1998 Safes and strongrooms provides advice on design criteria for safes and strongrooms (secure rooms) used to protect valuable physical assets.

It categorises safes and vaults as:

- basic — suitable for homes, small businesses, offices
- commercial — suitable for medium retail, real estate agents
- medium security — suitable for large retail, post offices
- high security — suitable for financial institutions, clubs
- extra high security (vaults only) — suitable for high-volume financial institutions.

The following international standards meet similar design criteria to the New Zealand Standard:

- BS EN 14450:2017 - Secure storage units. Requirements, classification and methods of test for resistance to burglary
- UL 687 - Standard for burglary-resistant safes

These international standards provide advice on testing for fire resistance in safes:

- UL 72 - Tests for fire resistance of records protection equipment
- JIS S 1037 - Standard fire test
- KSG 4500 – Fire-proof safes

Using secure rooms

Secure rooms are suitable for storing large quantities of official information or ICT in lieu of security containers. The minimum construction and security requirements for secure rooms are in the following classified documents (contact the PSR team for more information):

- NZSIS Technical Note - Class A Secure Room
- NZSIS Technical Note - Class B Secure Room
- NZSIS Technical Note - Class C Secure Room.

When you're selecting the minimum level of security for security rooms that will store official/protectively-marked information, you must use **this table**.

Visitor control

Follow clear, consistent processes for controlling visitor access to your facilities.

A visitor means anyone in a facility or area who:

- is not an employee
- has been granted access to the facility or area as a visitor.

This definition may include employees from other parts of your organisation.

Whichever entry control method you use, people should only be given unescorted entry if they:

- show a suitable form of identification
- have a legitimate need for unescorted entry to the area
- have the appropriate security clearance.

Augmenting visitor control with an electronic access control system

Visitor control is normally an administrative process. However, you can augment this process by using an electronic access control system (EACS). This allows you to issue visitors with EACS access cards enabled for the specific areas they may access.

In more advanced EACSs, it's possible to require validation from the escorting officer at all EACS access points.

Controlling visitor access to security zones

In security zones 3 to 5, you must issue visitors with visitor passes and record details of all visitors.

In zone 2, you should issue visitors with visitor passes and keep a visitor record.

Visitor passes must be:

- worn at all times
- collected at the end of the visit
- disabled on return if the passes give access to any of your access control systems
- checked at the end of the day and, when the passes are reusable, disable or recover any that haven't been returned.

One of your people should escort visitors.

You may, based on your risk assessment, record visitor details at the:

- facility reception areas
- entry to individual security zones.

Keeping a visitor register

Visitor registrations should be utilised by agencies.

Your visitor register should include the:

- name of the visitor and their signature
- visitor's agency or firm or, in the case of private individuals, their private address
- name of the employee to be visited
- times the visitor arrived and departed
- reason for the visit.

A visitor register should not be left unattended and should be held by a designated employee. This is often the person staffing the reception desk.

If your organisation manages access into specific areas at the entry to the area, those areas should have their own visitor registration process.

Visitors into zones 4 and 5 or sensitive areas should provide government-issued credentials embodying photographic identity features and a signature.

Removing people from your premises

You must have documented procedures for dealing with members of the public who behave unacceptably on your premises or who are present in a restricted area. Your people must be informed of these procedures.

If a member of the public behaves in an unacceptable manner, a duly authorised person should take the following steps when they consider it necessary for the person to leave the premises.

- Ask the person to stop the behaviour and warn them they could be required to leave the premises immediately.
- If the person does not stop the unacceptable behaviour, advise them that due to their behaviour, they no longer have permission to be on the premises.
- Ask the person to leave the premises immediately.
- Warn the person the police will be called if they remain, and of the possible legal consequences of non-compliance with the request to leave.

In most cases the person will agree to leave. If it is safe to do so, the person should be accompanied until they have left. However, if they refuse to leave, contact the police immediately.

No employee or guard is to attempt to physically remove a person from your premises unless permitted to do so under legislation. This would normally be left to a police officer. The contact number for the police should be available to all employees.

Relevant legislation may include:

- Summary Offences Act 1981
- Crimes Act 1961
- Defence Act 1990

Managing access to your premises by the media

If anyone in your organisation is considering giving access to media representatives, they should consult your chief security officer (CSO) before they grant access.

Add the following procedures to your standard visitor control procedures:

- a designated employee should accompany media representatives throughout the visit
- protectively-marked information should be locked away (preferable) or at least protected from view
- additional restrictions are considered when appropriate, such as handing in mobile phones and other recording and communications equipment

- your media liaison unit or public affairs area is consulted about the arrangements.

Additional controls may be necessary for particular sites.

If your organisation grants permission for a visit to areas where protectively-marked or private information is being used or handled, the employee responsible for the media representatives should remind them that no photographs or recordings of any type can be taken at any time during the visit, except with specific approval.

Access by children to areas where protectively marked information is stored or processed

Your organisation should develop policies to cover when children are allowed into areas where sensitive or protectively-marked material is held or used.

Parents or guardians are responsible for getting prior approval for children to enter official premises.

Remember to keep a log of children who enter in case there is an emergency situation.

Pre-school children

Pre-school children may be permitted short-term access if the parent or guardian (being a staff member):

- has approval from the relevant manager
- is with their child(ren) at all times.

Some pre-school children can read, but they're less likely to fully understand protectively-marked material than older children. They're also less likely to recall details, such as names and identities.

School-aged children

School-aged children are often able to understand written material and have well developed long-term memory. They should only to be allowed access under extenuating circumstances and only at the discretion of your organisation's chief executive or head.

Extenuating circumstances under which access may be granted are:

- a staff member is called in for emergency duty and no childminding is available at short notice
- a staff member is recalled from leave and a child requires unique parental care
- a staff member is required to sign papers, arrange posting activity, or other administrative tasks while in sole charge of a child
- normal childcare arrangements end without notice and a staff member, who is required to report for duty, is unable to make alternative arrangements
- a staff member is required to attend for duty when a child is injured (but not suffering from infectious illness) and requires monitoring.

The parent or guardian is responsible for the safety, wellbeing, and behaviour of the child while on the premises (including emergency evacuations). They must not to leave the child unattended, noting:

- children (as with any other uncleared individuals) must not be given access to corporate IT systems or protectively-marked material
- work areas should, as much as possible, be cleared of any sensitive or protectively-marked material while children are present
- children should not be present at meetings or during discussions where sensitive or protectively-marked material is discussed
- children who are suffering from, or convalescing after, an infectious illness must not be granted access (in line with occupational health and safety requirements).

Receptionists and guards

Control visitors and deter threats with receptionists and guards.

If your organisation has regular public or client contact, you should have receptionists or guards to greet, assist, and direct visitors.

Guards deter threats to information and physical assets and can provide a rapid response to security incidents.

Follow good practice

Receptionists and guards:

- should be able to easily lock all access to the reception and non-public areas in the event of an emergency
- may only perform other duties, such as CCTV and alarm monitoring, if it does not interfere with their primary task of controlling building access through the reception area. If performing other duties, they should be suitably trained and competent
- must be able to lock away all valuable or sensitive material (for example, paperwork, keys) if they need to temporarily leave the vicinity
- must have a method of calling for immediate assistance if threatened, for instance a duress alarm or radio, as they are most at risk from disgruntled members of the public
- must hold security clearances (and briefings) at the highest level of information to which they may reasonably be expected to have incidental contact with and in line with the facility with which they work.

Your organisation must:

- provide receptionists and guards with detailed visitor control instructions
- identify any security concerns for receptionists, guards, and people using your reception areas in a security
- risk assessment and mitigate concerns
- ensure that contracted guards are licensed under the Private Security Personnel and Private Investigators Act 2010.

Out-of-hours guarding

Guards and patrols may be used separately or along with other security measures.

Base your requirement for guards on the level of threat and any other security systems or equipment that are already in place. That will guide your decisions on what their duties are and how often they need to carry out patrols.

Security zone requirements

You can use out-of-hours guarding or patrols instead of alarm systems in zones 1 to 3. These guards may be permanently on site or visit facilities as part of regular mobile patrolling arrangements.

You must not use guards instead of an approved security alarm system in zones 4 and 5. However, guard patrols can be used as an extra measure.

You may use out-of-hours guard services in response to alarms in all zones. The response time should be within the delay period given by the physical security controls.

The highest level of assurance is given by 24 hours a day, seven days a week on-site guards who can respond immediately to any alarms.

Where guard patrols are used instead of an alarm system, patrols should be performed at random intervals. For zone 3, base the intervals on an your risk assessment but make sure they are within every 4 hours. For other areas, base the intervals on your risk assessment. For maximum effectiveness, patrol intervals and paths and timing should be random.

Where gurads are used to patrol inside a security zone, they should check all security cabinets and access points as part of their patrols.

Other physical security measures

Work out which other physical security measures your organisation might need to address specific risks.

Use the following examples to help you work out which physical security measures will best meet your specific requirements. (Note: This list is indicative not exhaustive.)

Measure	**Used to**
Hidden and/or fixed duress alarm	Address personnel safety concerns for reception areas and meeting rooms. May be of value for home-based workers
Individual duress alarm	Address personal safety concerns for personnel in the field or unpatrolled public areas
Individual item alarm and/or alarm circuit	Provide extra protection for valuable physical assets in your premises or physical assets on display
Vehicle alarm	Deter vehicle theft or theft of information and physical assets from vehicles

Two-person access system	Provide extra protection for extremely sensitive information
Vehicle safes	Deter theft of information and physical assets from vehicles
Vehicle immobilisation	Prevent vehicle theft
Front counters, and interview or meeting rooms	Restrict access by aggressive clients or members of the public. Allow regular meetings with clients or members of the public without accessing work areas
Mailrooms and delivery areas	Provide a single point of entry for all deliveries Prevent mail-borne threats from entering a facility without screening
Technical surveillance counter and audio security	Reduce vulnerability to, or detect, the unauthorised interception of information Reduce vulnerability to electronic eavesdropping on sensitive conversations
Conference security	Prevent unauthorised people gaining access to information or people and ensure the proceedings are conducted without disruption

Using vehicle immobilisation techniques

Vehicle immobilisation can reduce the loss of vehicles to theft. Vehicle immobilisation can be broadly divided into two types: automatic and remote.

With automatic immobilisation, a vehicle can be immobilised when not in use and requires a key or electronic token to start the vehicle

With remote immobilisation, a vehicle can be immobilised while in use and this technique is normally used along with a remote tracking and alarm system.

See also:

- Securely transporting sensitive items
- Vehicle alarms
- Fitting vehicle safes

Protecting front counters, and interview or meeting rooms

If your people interact with the public or clients who may become agitated, your organisation must install measures to reduce the risks to their safety.

These measures might include:

- a specialised front counter design that limits or delays physical access
- interview or meeting rooms monitored by guards or fitted with duress alarms (or both)
- interview or meeting room desks that act as a barrier
- reduction in items which could be:
  - thrown or used as weapons
  - used to aid climbing reception counters
- means of safe escape for staff to secured spaces or escape for visitors to public spaces
- separating key staff from public entry points

If your people regularly interact with clients or the public, consider establishing interview or meeting rooms that are accessible from your public areas.

See also:

- Visitor control
- Receptionists and guards

Reducing threats to mailrooms and delivery areas

Mailrooms and parcel delivery areas are areas of significant risk from chemical, biological and radiological attacks and improvised explosive devices.

Your organisation must assess the likelihood of mail-borne attacks and, if warranted, apply suitable physical mitigations. For example:

- mail screening devices
- a standalone delivery area
- a commercial mail receiving and sorting service
- separate or isolated air conditioning.

For help to select mail and parcel screening and handling equipment that meets your needs, try Australian **HB 328 Mailroom Security**.

Educate and train your people

Make sure your people are aware of your mail handling policies and procedures.

You must give your mailroom staff training – they must know your mail handling procedures and how to use any screening equipment you have.

Using technical surveillance countermeasures and audio security

Technical Surveillance Countermeasures (TSCM) is a process used to:

- survey facilities and detect any surveillance devices
- identify technical security weaknesses that could be exploited (including controls such as locks, alarms, and electronic access control systems).

TSCM provide a high level of assurance that sensitive information is free from unauthorised surveillance and access.

TSCM is mainly a detection function that seeks to locate and identify covert surveillance devices:

- before an event
- as part of a programmed technical security inspection or survey
- because of a concern following a security breach (for example, the unauthorised disclosure of a sensitive discussion).

When you must carry out a TSCM survey

Your organisation must carry out TSCM surveys for:

- areas where TOP S*CRET discussions are regularly held, or the compromise of other discussions may have a catastrophic business impact
- before conferences and meetings where TOP S*CRET discussions are to be held.

Seek advice from the Government Communications Security Bureau (GCSB) before you carry out a survey.

Protecting sensitive talks on the phone

To protect discussions about content that is protectively marked, your organisation must meet the logical controls in the New Zealand Information Security Manual - Telephones and Telephone Systems.

Managing security for conferences

Carry out a risk assessment before holding a conference to identify risks and mitigate them. If warranted, develop a specific conference security plan.

The aims of conference security should be to:

- protect the people attending the conference
- prevent unauthorised people gaining access to official information, protectively-marked information, or physical assets
- protect property from damage
- ensure the conference is not disrupted.

Also refer to Event security.