



9(2)(a)



On 16 October 2017, you emailed the Ministry with a request for the release of information relating to security at Work and Income sites, and your personal information. This response addresses your request for information about the Ministry's policies and procedures, under the Official Information Act 1982.

Before addressing your questions, in order to provide you with additional context about the information you have requested, I have provided you with some background information below.

Every week Work and Income sees 38,000 clients face-to-face. The vast majority of these interactions do not pose a threat to staff, and clients are able to be seen and assisted without any issues. However, as part of day-to-day work, staff see people who are vulnerable, who are frustrated, and who are managing complex personal situations. Occasionally these issues manifest in intimidating, threatening or inappropriate behaviour towards Ministry staff. The Ministry has zero tolerance of this type of behaviour and security guards help to make sure that the Ministry does not admit anyone who might represent a risk to the safety of other clients or Ministry staff.

Security enhancements were introduced to Ministry of Social Development Service Centres from 16 January 2017, and have since then been gradually rolled-out through the country. This enhanced process is referred to as 'Fully Controlled Access'.

The Fully Controlled Access process is not hugely different from what was happening before these new security measures were introduced. Information for clients about the process has been available for some time now, and is on the digital signage in site offices, on the Work and Income website and provided through Work and Income Contact Centres.

An important aspect of the Ministry's security is knowing who is coming into the Ministry's offices. Under the Fully Controlled Access process, a security guard on duty will typically have a list of appointments at the site as well as a list of those people trespassed from the site. If a person's name is on the appointment list, then they may not be asked for ID. However, I can assure you that not having ID or an appointment should not mean a person will not be admitted.

In a minority of cases when Fully Controlled Access was in its early stages, some people were refused entry due to not having ID. This was not the intent of security changes and Service Centre staff and security guards were reminded that people

should not be denied entry just because they do not have or do not provide identification.

I have enclosed for your reference copies of two documents that outline the standard operating procedures for the Ministry's security guards and the Fully Controlled Access guidelines for managers. You will note it is clear in both of the following documents that not having ID is not a reason for a site refusal:

- *'Protocols for Security Guards'*, dated December 2016.
- *'Fully Controlled Access – Towards future state office environment – guidelines for managers (FINAL)'*, dated January 2017.

Your questions are addressed in turn below:

- *NZ Police do not have the right to ask for ID unless there is suspicion of a crime. Can you point out where it is lawful for Armourguard security to demand ID prior to entry to a public building? (Internal policy isn't lawful) Also inline with informed consent what are my rights as a MSD client to refuse this request? What are my rights if I refuse a request and am not allowed entry? What lawful provision are Armourguard enacting to deny physical entry to a public building?*

The Ministry is entitled to restrict access to its work places and Armourguard is contracted by the Ministry to provide security. While public services are provided from Ministry workplaces, they are not public places and the Ministry has an obligation to ensure that the workers and others that use them are safe. The principal source of these obligations is the Health and Safety at Work Act 2015.

In addition to the above information, I can advise that people visiting a Work and Income office will be asked for identification – any form of identification. As not everyone carries identification at all times, if the security guards are satisfied someone does not pose a threat and has a genuine reason for visiting, the lack of identification or refusing to provide identification will not be a barrier to them coming into the offices, and clients have the right to refuse to provide identification.

If someone is refused entry to the office they can call the Ministry's 0800 number for the contact centre (0800 559 009) or utilise online facilities for assistance.

Information about how to make a complaint if you are unhappy or not satisfied with the Ministry's service is available on the Work and Income website here: www.workandincome.govt.nz/about-work-and-income/complaints/index.html.

On this webpage you will also find information about the complaints process, how complaints are investigated and what to do if you are not happy with the outcome.

- *What training have those Armourguard staff members on duty that day have in dealing with vulnerable persons?*

The enclosed document titled, *'Fully Controlled Access – Towards future state office environment – guidelines for managers (FINAL)'*, dated January 2017, includes a section outlining the specific training that security guards received in relation to the implementation of Fully Controlled Access. This training included health and safety briefings, working through scenarios, as well as opportunities to talk through any concerns they may have had, and discussion of frequently asked questions.

Security guards also watched a video titled '*Lives like mine*' to help them to empathise with some of the challenges faced by Work and Income clients.

Armourguard also met with all the guards to ensure they were clear about the Ministry's expectations and locally, site managers have daily briefings with all security staff to make sure security and Ministry staff are working together to provide a service while keeping everyone safe, including the Ministry's clients.

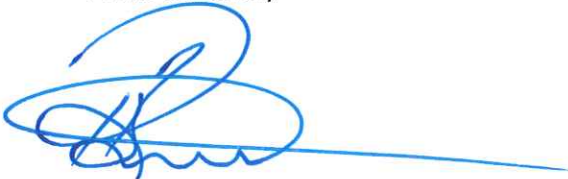
The Ministry has been working very closely with Armourguard to make sure their staff understand the new guidelines and get up-skilled. This includes ensuring that contracted security personnel are fully aware of their obligations under the Privacy Act, including using any private information provided strictly for the purposes for which it is required. The Office of the Privacy Commissioner is aware of the process the Ministry is using and is satisfied it meets the requirements of the Privacy Act.

If you are concerned about your privacy you have the right to complain to the Privacy Commissioner. Further information about how to complain is available on the Privacy Commissioner's website here: www.privacy.org.nz/your-rights/how-to-complain/

If you wish to discuss this response with us, please feel free to contact OIA_Requests@msd.govt.nz.

If you are not satisfied with this response, you have the right to seek an investigation and review by the Ombudsman. Information about how to make a complaint is available at www.ombudsman.parliament.nz or 0800 802 602.

Yours sincerely



Ruth Bound
Deputy Chief Executive, Service Delivery

Fully controlled access

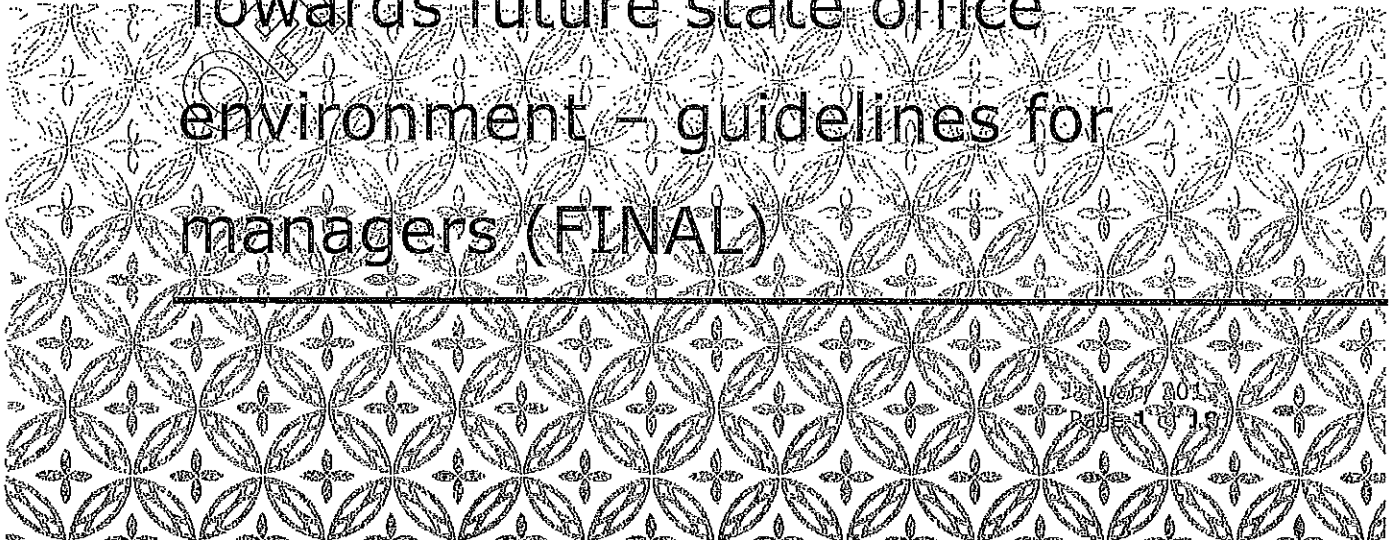


MINISTRY OF SOCIAL
DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

Fully Controlled
Access

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Towards future state office
environment – guidelines for
managers (FINAL)



Contents

Introduction	5
Fully controlled access	6
Fully controlled access - Guidelines	7
Frequently Asked Questions – Fully Controlled Access	8
Scenarios	10
Notes and Ideas	11
Scheduled Roll out Dates.....	12
Service Centre Readiness Report.....	13
Regional Readiness Report	15
Site Refusal Form.....	17

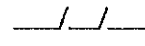
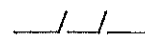
RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Sign off

This form records the approval and acceptance of the following document:

Document name	Version	EDRMS File reference
Towards future state office environment – Fully controlled access	FINAL	

The following signatures indicate approval and acceptance of the above document, subject to any caveats below:

Penny Rounthwaite	National Commissioner	
Caveats:		
Te Rehia Papesch	Associate National Commissioner	
Caveats:		

Contribution List

Version	Date	Author	Distributed to	Comments/Feedback
Version 1.0	11 November 2016	NC Team, Business Improvement Manager	National Commissioner Area HSS Property	Plan updated in a number of areas following meeting with Te Rehia Papesch, S 9(2)(a) Vaughan Crouch, Section 9(2)(a) Privacy of natural persons S 9(2)(a)

Fully controlled access

Version 2.0	30 November 2016	NC Team, Business Improvement Manager		Further feedback received from [§ 9(2)(a)] [§ 9(2)(a)] [§ 9(2)(a)], T Papesch, [§ 9(2)(a)]
Version 2.1	1 December 2016	NC Team, Business Improvement Manager		Update of FAQ's for Fully Controlled Access
Version 2.2	5 December 2016	NC Team, Business Improvement Manager	Associate National Commissioner Director Communications	Updated in a number of areas following meeting on 5 December 2016
Version 2.3	7 December 2016	NC Team, Business Improvement Manager	ANC, Director Communications RC's	Updated to include feedback
Version 2.4	8 December 2016	NC Team, Business Improvement Manager	National Commissioner Area HSS Property	Plan updated in a number of areas following meeting with Te Rehia Papesch, Melissa Gill, [§ 9(2)(a)] [§ 9(2)(a)] Vaughan Crouch, [§ 9(2)(a)] [§ 9(2)(a)]
Version 2.5	12 December 2016	Business Improvement Manager		Document split.
Version 2.6	14 December 2016	Business Improvement Manager		Further updates following feedback
Version 2.7	20 December 2016	Business Improvement Manager	ANC, HSS	Confirmation of roll out dates
Final draft	21 December 2016	Business Improvement Manager	NC DCE SD	Further updates
FINAL	11 January 2017	BIM	NC	Final Updates

Introduction

We're introducing two physical safety and security enhancements for front facing service delivery sites now.

What does this mean to you?

1. We are moving all front facing service delivery sites to fully controlled access (based on the model operating in the Canterbury Region). This isn't hugely different to what we are doing now, most sites already have guards opening the door, however guards will be engaging with each person as they enter the site; and
2. We will be asking you to move staff and reposition things (where practicable) so clients are seated opposite case managers (to create a delay) as opposed to beside and also look at what you can do to provide staff with clear exit routes from interviewing desks and if necessary, from a client who poses a risk. There are separate guidelines regarding repositioning.

Why now?

We are always reflecting on things we've learnt, and this is no different. This is an enhancement of what we already do and will ensure that we are all consistent including our guards. It also provides us with an opportunity to relook at how we work and set up our sites. This is important for our clients too, when they approach our sites they should expect a consistent service from our guards.

When will this happen?

Fully controlled access

Armourguard have taken action to upskill their staff however before they can fully implement we need to ensure that each site and each region is ready too. This will include talking with your teams and working with your guards to ensure they are feeling supported and comfortable with the changes. Working in partnership with your guards is a key success factor. If you have any concerns talk to the Health Safety and Security Team.

Some sites may have issues due to their physical limitations. In these cases, we need to be practical about how and what can be implemented. These limitations can be recorded in the Readiness Reports.

There is a four week window for implementation which will commence from 16 January 2017. Roll out will be staggered by region commencing in the South Island moving through to the top of the North Island. Regions will need to provide their Readiness Report sign off prior to implementation.

Each day we will debrief with the regions to ensure everything is going ok and discuss any issues that may have arisen.

Fully controlled access

The move to fully controlled access is an extension of the way we've successfully managed security in Canterbury over the past two years. This is also an opportunity to share and implement best practice which we have learnt from Canterbury.

We're asking security guards to have a conversation with people before they come into our offices. It's an opportunity to check if the person has a business reason to enter, that they haven't been trespassed, and helps to make sure we don't admit anyone who might represent a risk to the safety of other clients or our staff – for instance, if the person is intoxicated. It will enable site security staff to recognise potential incidents earlier.

Not having ID won't mean people can't come into a Work and Income office.

These conversations already happen at many of our offices, but we want to make sure that we apply this approach consistently across the country.

We're here to help people in times of need, but we won't place our staff or other clients at risk. We'll monitor the planned changes as they're introduced and respond quickly if any issues arise.

The insights from point-of-entry conversations by guards, particularly with clients who do not have scheduled appointments, provides the opportunity to escalate potential issues to site management, or where appropriate deny access.

As you know, the relationship you have on site with your security guards is extremely important to the on-going success of our service. We have put a checklist that should assist you and this is on Page 7.

Please take the time to show all security guards the "Lives like Mine <http://doodle.ssl.govt.nz/whats-on/news/celebrating-our-people/2016/lives-like-mine-empathy-makes-the-difference.html> video to help them understand some of the issues our clients may have. Also, discuss with them the FAQ's and scenarios contained in these guidelines.

Spend some time talking about this with your teams. If there is a scenario or question that comes up that you have resolved, record it and your solution and let your Regional Director know. These can be shared throughout the regions.

Fully controlled access - Guidelines

- All service centres (apart from smaller ones) will be staffed with a minimum of three security guards. One is to be based outside the main public entry door, or in the airlock. One should be inside the site controlling entry and exit. The third guard should be walking the service centre floor ready to assist staff if required.
- Fully controlled access means the main public entry door to your service centre is locked, opened by a security guard once they are satisfied the client, visitor, contractor or other agency staff has legitimate business there and does not pose a risk. The main entry door must **not** be on 'automatic' so people can freely wander in.
- If an incident occurs inside the service centre, the security guard controlling the door needs to unlock it immediately in case the manager decides staff and clients need to leave the site. In some cases it may be safer for staff to use an alternative exit to the front doors, i.e. back door or side exit. Follow the instructions of your manager.
- Each morning, security guards controlling access to your service centre should be given a list of the names of clients, visitors, contractors, etc who have appointments, or are expected that day and an estimated time window for arrival.
- The guard needs to be reminded that the list is sensitive and needs to be treated with a high level of care. Provide a clip board with a top cover to your guard to keep the list secure.
- This list should be printed on plain or unbranded paper.
- All visitors (clients, staff, contractors, other agency staff) to your service centre should be greeted by a guard and politely asked why they wish to enter the site.
- All MSD staff will carry ID so their entry to your office should be straightforward.
- All clients should be asked politely to provide ID. This quick interaction allows the security guard to assess if there are any immediately apparent reasons why they shouldn't be allowed into the site. It may also help identify a client who has been trespassed.
- This ID can be checked against the list the guard holds.
- Some clients will not have identification. They can be asked to provide letters/etc. from Work and Income or other agencies.
- Visitors who do not have any form of ID, but have an appointment, will appear on the visitors list the security guard has. Once the guard is satisfied the person doesn't appear to pose a risk they can be admitted to the site. The guard should remind the client to bring ID the next time they visit.
- The security guard can still admit clients and visitors without ID and appointments to the service centre once they are satisfied that they don't appear to pose a risk.
- Clients shouldn't bring skateboards, scooters or bikes into the service centre. They should be locked outside. If they can't be left outside, they can be left in the lobby where they don't cause a hazard or would act to prevent people leaving the building in the event of an emergency (fire, earthquake).
- Where a client is refused entry the guard will need to complete a Site Refusal Form. Even if we do not know the client, the details should still be recorded. The time of the incident should be recorded as well.
- New guards to your site will need to be briefed about our expectations and process. Please do not leave this to the existing guards. As the site manager you must take responsibility for this. There should be a clear plan of who is responsible to do this in your absence.

Frequently Asked Questions – Fully Controlled Access

Is fully controlled access about ID and whether they have an appointment?

ID and an appointment is a supporting feature of fully controlled access rather than a defining feature. Whether the person has an appointment or not, or ID or not, is not the significant factor. It is how they present when they come to the site. The door remains closed and is only opened when the security guard has made an assessment that the person is fit to enter the site. The fitness considers factors such as:

- Whether the person is intoxicated or highly agitated
- Our history with the client

Will people be turned away by the security guards if they don't have ID?

No. A person will be turned away if they appear to pose a risk.

We are at a co-located site; will we stop their clients too?

The Manager should discuss the process with any co-located stakeholders and other agencies and make them aware of our move to fully controlled access and what that means for them. It is important that we reiterate that this is not about stopping people from coming in, having the right ID or about having an appointment. Controlled access needs to operate consistently in all sites.

Is there any signage?

There is no plan to have printed information to service centres however appropriate digital messages will be added to kiosks and digital signage screens.

Is the contact centre aware of the move to Fully Controlled access?

Yes, they are aware. The Contact Centre will continue to advise clients that they need to bring ID with them when they visit our sites.

Our site doesn't have electronic doors which means opening and locking the door each time a client comes in or goes out. This will create problems and potentially increase aggravation from clients. What do we do?

If you have issues with unlocking and locking the door make sure you record this on your Readiness Report which you need to send to your Regional Director. This will form part of the Regional Readiness Report. We will escalate the initial issue to Property.

On a Wednesday, there is usually a queue of clients and in some cases over 20. How would we manage this?

From what we learnt in Canterbury, their receptionist and one case manager leave the weekly training 10 minutes early and they work with the guards to give entry to clients so that they are ready at 9.30am for case managers to pick up.

This is a different role for our guards, will they get training?

Yes, Armourguard will be meeting with all the guards to ensure they are clear about our expectations. Guards will continue to have a daily morning briefing.

The Service Centre Manager will also show the "Lives like Mine" video and take the guards through the FAQ's and scenarios in this document.

Can you ensure people won't have a bad experience?

Armourguard are training their people and our managers will have a daily briefing with guards so expectations are very clear before we open the doors. All clients who don't pose a threat and have a legitimate reason for being at the site will be able to access our services. The Contact Centre will reiterate the same messages; the Service Centre Manager is talking with any co-located people.

What information should be contained on the daily appointment lists?

As a minimum, you should have recorded the clients' name and appointment time. If possible, do not include the SWN on this document.

What do we do with the daily appointment lists?

The daily appointment list can be destroyed however the Site Refusal forms should be checked by local staff, scanned and sent to your regional office. They will collate and send to the National Commissioner team. The National Commissioner team will record and retain the information.

Is it a privacy breach giving the names to the guard?

No, there is no privacy breach in sharing this information however if the guards use the information outside of the purpose it was intended for, this would be considered a breach. Armourguard would manage this.

What happens if the guard loses the daily list?

This should be treated the same as a privacy breach. Since Canterbury has been on fully controlled access there have been no incidents of this kind.

Appointments can be made on the day by the Contact Centre or other staff in the site. How do we update the Appointment list?

Fully controlled access is not about checking off clients against an appointment list. Clients may call into the office without an appointment. There is no formal need to update the Appointment list. If a case manager believes that the client may become agitated with the process or may be distressed by the process they should let the guard know this.

The guards are unable to communicate easily with each other. Is anything being done to address this?

Currently we are testing the use of ear pieces for guards at the Willis Street, Levin and Porirua sites. We will be watching their progress and may extend these further.

How will the guard know if a client has been trespassed?

Currently, each region has a Trespass Notice Register. Each region needs to share this with each of their sites on a regular basis. This will be provided to the guard who will also have the daily list. Regions should update this register weekly.

We are having problems with our guard/s and they are not meeting the standards.

If you have any issues with your guards you should contact your Regional Director who will liaise with the regional Armourguard person and discuss it with them. If you are not satisfied, please escalate further to S 9(2)(a).

Scenarios

We have provided some FAQ's and there are many scenarios that could occur. Here are some that may help you and your guards.

Scenario	Action to take
Client approaches service centre wanting to come in but has no ID or appointment booked. Client will not give the guards their date of birth or anything to identify themselves.	Having no ID or an appointment is not a reason to be refused entry. If the client behaves in a way that poses a risk they should not be permitted to enter however the guard will need to determine this. If the client is refused entry, their details should be recorded on a Site Refusal Form.
Client presents at a service centre and appears under the influence of alcohol.	Under no circumstances should the client be given entry to the site. Their details should be included in the notes made to the Daily Appointment list.
Client calls at the office and has walking sticks. These could be considered weapons	If the client presents at the office and is using walking sticks and they need these for their mobility the client should be vetted as per the normal procedures and allowed to enter the site.
There is a queue of people waiting to get in to the service centre	We should still maintain the entry process and the guard will need to talk with each client. All our appointments are staggered, this will help reduce this issue.
A client is refused entry to an office and they must attend an appointment e.g. sanctioned if they don't attend the meeting	We don't want clients to be sanctioned if they have made a genuine attempt to see us however if a client behaves in a way that poses a risk, they should not be permitted to enter the site. We understand that failing an obligation may mean a form of sanction. The guard will complete a Site Refusal Form and at the end of each day the manager should have a quick discussion with the guard about any issues that may have arisen during the day. If the clients name was recorded, the manager will be able to pass these details on. If a staff member was expecting a client and their non-attendance would mean a sanction is imposed, the staff member should try to contact the client by phone. The staff member can check the Site Refusal Form details however this would need to be at the end of the day when the guards are not on duty. Don't impose the sanction, allow another attempt for client to comply.

Notes and ideas

Manager meets with all guards every morning

Debrief from previous day (if not done previous day)

Provides guard/s with appointments list for the day (exclude SWN's)

Provide guard/s with trespass notice register

Discuss any potential issues, reiterate expectations. (An idea might be to have a book and all discussions are recorded in the book.)

Manager provides details of refusals to Regional Director

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Scheduled Roll out Dates

Initially, we were going to roll out every site and region over a prolonged period however this posed logistical problems for Armourguard and also increased the potential risks to the organisation especially if clients were going from site to site and encountering different access procedures.

Following the implementation in each region, the National Commissioners office will teleconference with each of the Regional Directors and discuss any issues or problems that may have arisen during implementation.

Region	Date of implementation
Canterbury	16-Jan-2017
Southern	17-Jan-2017
Nelson	18-Jan-2017
Wellington	19/1 - 20/1/17
Central	23/1 - 25/1/17
Bay of Plenty	26/1 - 27/1/17
East Coast	2/2 - 3/2/17
Taranaki	7/2 - 8/2/17
Waikato	9/2 - 10/2/17
Auckland	13/2 - 15/2/17
Northland	16/2 - 17/2/17

Service Centre Readiness Report

This report provides assurance to your Regional Commissioner and Regional Director that your site is ready to implement the **fully controlled access** changes and that any issues have been identified and plans are in place to address these.

Please return electronically to your Regional Director before your regions scheduled roll out date.

Service centre:	
-----------------	--

Category	Description	Yes/No	Add comments
Guard	Guards have been taken through FAQ and scenarios		
	Guards have a clear understanding of fully controlled access		
	Guards have completed Armourguard training		
	Guards have watched "Lives Like Mine" Video		
Your Team	All staff have been briefed		
	All staff have worked through the FAQ's and scenarios		
	All staff have a clear understanding of fully controlled access		
Your site	Can you implement fully controlled access? If no, please record the reasons why.		
	Are you co-located? Have you met with your stakeholders in your shared site and explained this?		

Readiness confirmation statement

1. <Service Centre> is fully prepared for the implementation of fully controlled access.
2. All regional deployment deliverables and activities will be completed by _____
<Date prior to scheduled roll out>
3. Regional implementation date has been agreed.
4. Deployment risks identified by the region have been mitigated or escalated.

Yes/No. If 'no' indicate why (if applicable):

Signed by: Service Centre Manager <NAME>	Dated:

Email completed report to the nominated Regional Director contact.

Regional Readiness Report

This report provides assurance to:

- **DCE, Service Delivery**
- **National Commissioners**
- **Health Safety Security**

That your Region is ready to implement the fully controlled access enhancement and that any issues have been identified and plans are in place to address these.

Please return electronically to § 9(2)(a) two days before your Implementation Date.

Region			
Category	Description	Yes/No	Add comments
Communications	Service Centre Managers (SCMs) have met with Security Guards and completed scenarios		
	All guards have watched the Lives Like Mine Video		
	In co-located areas, SCM has met with key stakeholders e.g. community link, partners, building tenants and discussed implementation		
	Co-located stakeholders have a clear understanding of fully controlled access.		
Staff	All staff have been briefed on fully controlled access		
	All staff have worked through the FAQ's and scenarios		
	All staff have a clear understanding of fully controlled access		
Sites	All sites are able to implement fully controlled access (Record any exceptions and reasons why)		
	Staff know how to escalate issues.		

Fully controlled access

Readiness confirmation statement

- 5. <Region> is fully prepared for the implementation of **fully controlled access**.
- 6. All regional deployment deliverables and activities have been completed by our go-live date
- 7. Our regional implementation date is <Date>.
- 8. Deployment risks identified by the region have been mitigated or escalated.

Yes/No. If 'no' indicate why (if applicable):

[Empty box for response]

Signed by: Regional Commissioner <NAME>	Dated:

Email completed report to S 9(2)(a) @msd.govt.nz

Site Refusal Form

This form must be completed by the guard when a person is refused entry to any site.
 Return to the site manager with the Daily List.
 Any physical altercations must be recorded using the Incident Management reporting.

Date	
Guard	
What time were they refused?	
What was the reason for refusal?	<input type="checkbox"/> Abusive behaviour <input type="checkbox"/> Intoxicated <input type="checkbox"/> Under the influence of drugs <input type="checkbox"/> Intimidating behaviour <input type="checkbox"/> Threatening (Please record details below) <input type="checkbox"/> Other (Please record details below)
What happened? Please write down as much information about what made you refuse entry to the person.	[Large empty space for text entry]
Do you know the person's name? If you know their name please write this down.	Circle One: Yes / No / Not able to ask
Did they have an appointment?	Circle one: Yes / No / Not able to ask

RELEASED UNDER THE INFORMATION ACT

Protocols for Security Guards

1. Function of Security Guards

The prime function of the security guard is to observe, monitor and report for the purposes of ensuring the safety and wellbeing of MSD employees and clients.

2. Requirements for Security Company

The image guards' project reflects on both their company and the Ministry, therefore the following standards have been put in place.

The security guard company will ensure all guards deployed for MSD purposes:

- Hold and display on site a NZ Security Guard Certificate of Approval
- Meet MSD vetting/background standards before they are deployed
- Receive appropriate training in the roles and functions they are to carry out for the Ministry
- Have undertaken the security companies basic training on Customer Service and Conflict Management
- Display a high standard of professionalism; be clean, tidy, well-groomed and in full uniform
- Have completed security company's induction of hazard identification and controls training and have immediate access to hazard reporting documentation
- Have a competent ability to communicate in English
- Perform their duties in a manner that is courteous, polite, helpful and considerate to others
- Be alert and immediately ready to assist
- Must not leave the site for any reason unless directed to by your Supervisor or escorting a staff member to their vehicle as directed by Site Manager
- Conduct welfare checks with Armourgard Welfare Department as required

3. Requirements for Ministry of Social Development

MSD are to ensure all guards deployed on site:

- Receive a full site Health & Safety induction including any identified hazards and risks and noted in the site Health & Safety folder
- Receive a full site security orientation including; site procedures which includes emergency management outlined in the Site Safety Plan, CCTV monitors, locking systems on all doors and windows, duress and evacuation system and procedures, lock down procedures, alarm monitoring emergency contact list, duress pendant register
- Attend the site 'start-up brief' at the start of each day to ascertain from site management if any known risks or concerns have been identified for that day. Guards must be reminded that this information is sensitive and needs to be treated with a high level of care.

4. Guard responsibilities

Duties may vary to suit changing needs but they should not detract from the primary purpose of keeping staff and other clients safe. The list below is not exhaustive but the guard may:

- Be proactive in the identification and reporting of potential health, safety and security hazards in the work environment
- Liaise with the site manager to identify if there are after hours (5pm) security requirements where MSD clients may remain onsite
- Ensure that all emergency exits are clear
- Be involved in the planning and monitoring of interviews where there is the potential for conflict
- Move around the office and be visible but discreet in the role of Internal roaming guard

MSD Guard Standard Operating Procedures - Final December 2016

- One of the guards on site to be a member of the Health and Safety committee
 - Respond as appropriate to any duress alarm or emergency situation that may occur on site
 - Patrol other areas of the building (where the Ministry has a presence) as directed by the Site Manager
 - If requested by the Site Manager escort staff to their vehicles
 - Manage the visitors book (where applicable)
 - Assist in checking that Security, Visitor and Contractor identification is worn
 - Report all tasks in the site activity log
 - Report all/any security and safety concerns, activity and/or incidents
 - to the site manager;
 - by way of Incident report and escalate accordingly
 - if in doubt report and seek guidance from your supervisor
5. Place the site into lock down if there is a clear and present danger that is required to be mitigated
6. Tasks guards will not undertake:
- Photocopy or handle client files, open mail or conduct any filing of client information under any circumstances
 - Be responsible for holding onto or storing any clients' personal property
 - Be responsible for reception duties
 - Be responsible for general cleaning duties i.e. cleaning staff room, un/loading the dishwasher
 - Be sent off/leave site for any reason other than a staff escort to the car park
 - Serve trespass notices off site on behalf of the Ministry
 - Checking of any Staff Car Parks excluding escorting staff to their vehicles
7. Managing conflict:
- Site Managers need to be aware that guards only have the same rights as any other member of the public when dealing with conflict. As such, when dealing with conflict on site the guard will be acting as an agent for the Ministry under the direction of the Site Manager. Accordingly, the guard needs specific authority from the Site Manager if they are required to ask a person to leave and/or trespass them from the site.
 - The guard is required by law to warn the person that they are acting on the authority of the Ministry of Social Development and they must leave. The person is then to be given adequate time and opportunity to leave the premises without the use of force. If the person refuses to leave, or becomes aggressive or violent the guard may use the minimal amount of force as is required to remove the person from the building.
 - If a situation occurs whereby it is realised a person is refusing to leave the site and/or is becoming aggressive or violent the Police should be contacted via 111.
 - In the event of any person being requested to leave a Ministry of Social Development site, such an event must be reported to the guard supervisor then recorded and forwarded as an Incident Report
8. Incident Report
- Incidents are required to be documented by the guard as soon as practicable after an incident. This will be done by way of an Incident Report
 - The incident is required to have been verbally reported to the Site Manager initially and the detail of the incident documented in the Incident Report
 - The Incident Report must be signed by the guard and maybe signed by the Site Manager

MSD Guard Standard Operating Procedures - Final December 2016

- A copy of the Incident Report is scanned/faxed to the regional Armourguard branch as soon as completed
- As directed in the Incident Report, verbal notification to your supervisor and/or Armourguard Welfare Department may be required

The following are examples of where an Incident Report is required to be completed:

- Any assault on Ministry of Social Development staff, guard(s), and/or clients
- Any use of force by any guard on any person at any time
- Any incident where Police have been called to attend
- Any injury/medical or fatality event
- Any verbal abuse towards any person where the guard is involved
- Any alarm activation or security system issue
- Any warning issued to any client where the guard is involved
- Any weapons produced or observed upon any person
- Any hazard or risk in the site
- Any trespass notice issued
- Any building evacuation
- Any damage observed or created due to a client, Ministry of Social Development staff, visitor or guard
- Any threat of any kind to the site and/or guard, client or Ministry of Social Development staff
- Any time the site goes into lock down
- Any aggressive behaviour made by any person to any other person
- Any time a person is escorted from site for any reason
- Any other incident deemed Incident Report worthy not listed above

If guards have any doubt, they must report and seek guidance from their supervisor immediately.

9. Armourguard Welfare Department Escalation

Guards will escalate all available information to Armourguard Welfare Department as directed in the Incident Report.

- Immediate and/or critical support is required
- Any assault on Ministry staff, guard(s), and/or clients
- Any use of force by any guard on any person
- Any use of force by any Ministry staff on any person where the guard is involved in the incident
- Any incident where Police have been called to attend
- Any injury/medical or fatality event
- Any weapons produced or observed upon any person
- Any building evacuation
- Any time the site goes into lock down

10. Action to take if a weapon is observed in possession of another within the site

The entrance guards should have detected any weapon in the possession of any person and denied entry. However, in the event a weapon is observed in possession of another within the site follow the principle that human life is paramount; take no action that will endanger life or make the situation worse.

DO NOT CONFRONT THE PERSON IF YOU CAN AVOID IT

Take the following action:

1. Attempt to discretely keep the person under constant observation
2. Quietly and discretely ensure Police are called on 111
3. Inform the Site Manager and follow any directions given
4. Ensure the safety of yourself and people in the area and consider isolating the armed person by moving others discretely to a secure/safer position.
5. Position yourself in a safe location to observe and monitor the person and try to maintain the safety of others from that person.

TRY NOT TO BRING ATTENTION TO THE PERSON IF POSSIBLE

AWAIT POLICE ARRIVAL

6. Contact Armourguard Welfare Department and inform them of the situation.
7. Complete an Incident Report

10. Levels of Operation on Site

Each site will operate at any time under one of the following two (2) models.

A. Controlled Entry

Controlled Entry means that the main public entry door to the site is opened by the security guard once the guard is satisfied the client, visitor or contractor has legitimate business there.

- The door must not be on automatic entry at any time
- A list of booked appointments is to be provided to the External Guard by the Site Manager. This list should not be printed on MSD or Work and Income branded paper. Guards are to be reminded that the list is sensitive and needs to be treated with a high level of care and returned to the site manager at the end of the business day.
- All visitors to the site should be greeted by the External Door Site Guard and politely asked why they wish to enter the site.
- Clients with appointments are to access the site once the security guard is satisfied they do not appear to pose a risk
- Identification of all clients approaching the site is to be requested and verified before they are allowed to enter
 - Some clients will not have identification. They can be asked to provide letters/documents/etc. that have been issued by Work and Income or other agencies that verify their name. Clients who do not have any form of identification, but have an appointment, will appear on the visitors list the guard has. Once the guard is satisfied that they do not appear to pose a risk (i.e. they are not intoxicated or angry etc) they can be admitted to the site.
 - For those clients who do not have any identification and do not have an appointment the Security Guard can admit them to the site once they are satisfied that they do not appear to pose a risk.

MSD Guard Standard Operating Procedures - Final December 2016

- o For visitors (excluding clients) who do not have any identification, the staff member they are coming to see can be contacted by a guard to come and greet their guest.
- o For all persons denied/refused entry, the guard will complete the Site Refusal form and provide it to the Site Manager

B. Lock Down

1. Lock Down's may result when:
 - a. An imminent threat is made towards the site and/or staff member/guard/member of the public
2. No people other than emergency personnel are allowed to be let into the site
3. Clients/staff may be allowed to leave the site after a discussion with the site manager who will explain the risks to them if they leave the site.
4. A guard, if identifies an imminent risk, can place the site into Lock Down
5. The guard must immediately notify the Site Manager of the Lock Down and the reason/s as to why

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

MSD Guard Standard Operating Procedures - Final December 2016

Guard deployment model

All guards will rotate through all positions during the course of each day. This rotation is expected to be hourly, but may be more frequent depending on weather conditions.

The External Site Security Guard will be in place throughout opening hours.

External Site Security Guard	
Task	Action
<p>Tone and Treatment - <i>Messaging</i></p>	<ul style="list-style-type: none"> • Acknowledge all persons entering the site in a friendly and professional manner • Ask the client to remove inappropriate headress such as hoodies and helmets • This messaging is supported by signage • Consider religious headress and attire e.g. burka/turbans (if in doubt seek the advice of the Site Manager) • Consider religious/cultural/seremonial items (if in doubt seek the advice of the Site manager)
<p>Control Access</p>	<ul style="list-style-type: none"> • The door must not be an automatic entry at any time • Each location will need to assess 'best practice' in relation to door control i.e. sites with automatic doors may need to be opened from the inside, therefore two guards will be required to man-the-door at all times • The guard must be satisfied that the client does not appear to pose a risk (i.e. they are not intoxicated or angry etc.) • The guard will greet each person as they approach the site and request their ID and if the person has an appointment i.e. good morning, do you have your ID and an appointment with us today? • Some clients will not have identification. They can be asked to provide letters/documents/etc. that have been issued by Work and Income or other agencies that verify their name • There may be some instances where the client has no ID, if this occurs, if the guard believes they pose no risk to the site and have a genuine reason for being there they can be admitted to the site. • For visitors (excluding clients) who do not have any identification, the staff member they are coming to see can be contacted by a guard to come and greet their guest. <p>A list of booked appointments is to be provided to the External Guard by the Site Manager. This list should not be printed on MSD or Work and Income branded paper. Guards are to be reminded that the list is sensitive and needs to be treated with a high level of care and returned to the site manager at the end of the business day.</p>

<p>Intoxicated people</p>	<ul style="list-style-type: none"> Refuse entry to any person that appears to be intoxicated, under the influence of drugs or behaves erratically. 	<ul style="list-style-type: none"> Note - some medications may cause a client to present as under the influence Staff should identify clients from their daily appointment lists and provide you a 'heads-up' about these clients during the daily brief Any denied/refused entry is reported by way of a Site Refusal form
<p>Monitor client behaviour</p>	<ul style="list-style-type: none"> Scan each person to determine potential threat (concealed weapon/item capable of being used as a weapon) 	<ul style="list-style-type: none"> If you have any concerns about a person's behaviour: <ul style="list-style-type: none"> Request their ID Ask them for their reason for visiting If you have any concerns, refuse entry and suggest they phone the 0800 559 009 number to request assistance Any denied/refused entry is reported by way of completing a Site Refusal form. If the client becomes threatening, the Police must be contacted. Under no circumstances are staff to provide coverage to guards
<p>Maintain visibility</p>	<ul style="list-style-type: none"> Breaks must be managed between the guards, with a guard to be positioned outside at all times 	

CONFIDENTIAL UNDER THE INFORMATION ACT

MSD Guard Standard Operating Procedures - Final December 2016

Internal Door Site Security Guard		
Task	Description	Action
Tone and Treatment Messaging	<ul style="list-style-type: none"> To treat all people with respect and courtesy. 	<ul style="list-style-type: none"> Acknowledge all persons in the site in a polite manner.
Control Access	<ul style="list-style-type: none"> Maintain client flow through the manual open/close of the front door (if two guards are required). 	<ul style="list-style-type: none"> Each location will need to assess 'best practice' in relation to door control. i.e. sites with automatic doors may need to be opened from the inside. In these cases a guard must remain by the door at all times, and in the event of an incident inside the office, the door must be opened immediately.
Environmental Scan	<ul style="list-style-type: none"> Observe client/staff interactions and behaviour (e.g. Raised voices/swearing) 	<ul style="list-style-type: none"> Intervene in all cases where any person displays inappropriate behaviour Escort the client from the building immediately (if required/requested by Site Manager) Contact the Police if appropriate
Site Coverage	<ul style="list-style-type: none"> Provide cover for front door guard 	<ul style="list-style-type: none"> A guard must be present at the front door at all times Staff are not to provide coverage at any time Each site will need to assess best practice for managing breaks for Internal Door and Internal Roaming guard
Managing an incident on site	<ul style="list-style-type: none"> Manual door entry - Ensuring safety on the inside of a site 	<ul style="list-style-type: none"> If the door is controlled manually, a guard must remain by the door and open it allowing free egress from the site. * see below

*In the event a client becomes angry or aggressive whilst on site, all staff will avoid confrontation and make every effort to keep calm, stay safe and avoid unsafe situations. A guard will remain by the door and open it to allow free egress from the site. The site may then be placed into Lock Down as directed by the Site Manager.

MSD Guard Standard Operating Procedures - Final December 2016

Internal/ Roaming Site Security Guard	
Task	Action
<p>Tone and Treatment – Messaging</p> <ul style="list-style-type: none"> Treat all people within the site with respect and courtesy 	<ul style="list-style-type: none"> Acknowledge all clients within the site in a friendly and inviting manner
<p>Incident Prevention</p> <ul style="list-style-type: none"> Be involved in the planning and monitoring of interviews where there is potential for conflict 	<ul style="list-style-type: none"> Each location will involve the guard in their daily start-up brief Move around the office and be visible but discreet Respond as appropriate to any duress alarm or emergency situation that may occur on site
<p>Environmental Scan</p> <ul style="list-style-type: none"> Observe client/staff interactions and behaviour (e.g. Raised voices/swearing) 	<ul style="list-style-type: none"> Intervene in all cases where any person displays inappropriate behaviour Escort the client from the building immediately (if required/requested by Site Manager) Contact the Police if appropriate Complete an Incident Report
<p>Relief</p> <ul style="list-style-type: none"> External guard needs urgent relieving 	<ul style="list-style-type: none"> Urgent Situations may arise i.e. client demands to see the Manager where the external guard must talk with the Manager. In these cases, the Internal Roaming Site Guard should relieve them so that the guard can consult with the Manager