Thompson and Clark, Site Security Assessment, 24 August 2015

Feedback collated from ███ and Sarah

No	Recommendation	Comment
1	Support Services Manager security role to be defined within job description.	Agree
2	Develop Security Risk assessment programme to maintain a current understanding of the risk to the business and its personnel.	Agree
3	Develop and fully document baseline security performance criteria and ensure all staff and 3rd Party organisations use company security policy and procedures	Agree
4	Develop a site specific office security plan and introduce it to new employees as part of their induction.	Agree
5	Develop and maintain security operating level procedures with input from Thompson & Clark and manage on a weekly basis dependent upon threat level, publish or post these for staff members on a regular basis.	Agree
6	Introduce an auditing programme on the two Access Control Systems for the main building and for the internal doors on a quarterly basis to determine any old cards still active in the system and reaffirm appropriate access of existing personnel.	Agree
7	Conduct an audit on the two ACS on a quarterly basis to determine which employees have accessed the building outside of normal business hours on a regular basis. This could be achieved by exception reporting provided daily when out of hour's access has been made.	Agree
8	Develop a challenge culture within the organisation through written and scenario based training.	Agree. Security training conducted with all staff and scheduled to be conducted every 6 months. When specific incidents occur these are openly discussed at team meetings as a learning opportunity.
9	Security personnel should coordinate with reception when taking toilet or other breaks	Agree
10	Remaining security personnel that haven't had First responders training should receive this presentation to reinforce their understanding of the trespass act and section 56 and the expectation upon them during a panic	Agree
11	Update the current book with current relevant photos identifying problem claimants	Agree, this is reviewed on a monthly basis with the key staff at SR and updated as required.
12	Develop property inspection and search procedures and guidelines and integrate into the company employment agreements, contractor agreements and	This is not part of our employment agreements currently and would require consultation and discussion with staff before considering whether

	visitor sign in books.	to implement.
13	Develop documentation and procedures for company property removal off site	This recommendation requires further discussion as a considerable amount of information is available via the internet as a number of our systems are internet based (EMS, iViis, Aconex) Is logging in and out going to be practical? The guideline regarding security of paper files is covered under the SR Privacy policy.
14	Develop mail procedures and awareness training, all incoming mail including parcels should be channelled through the security guard at number 6 Show Place.	Agree with training and development of procedures around handling mail however not practical to have the security guard involved. The security guard needs to remain at the entrance and focussed on those coming into the building.
15	Consider restricting general staff access times to the buildings at number 6 and 10 to be between normal business hours.	This is already in place. Staff only have 24/7 access to their own floor. Only the executive team of Arrow and SR have 24/7 access to all floors.
16	Conduct annual refresh training in respect to tailgating reinforcing a challenge culture within the organisation.	Agree, training has been delivered and is scheduled to be conducted on a 6 monthly basis.
17	Request consultation with the landlord Goodman Property Service as to the suitability of future prospective tenant for level 3 of #10 and any conflict or risk towards SRES is considered.	The Landlord keeps us informed of the progress on security tenants however who they are negotiating with is confidential as it is commercially sensitive.
18	Outside of normal business hours this rear door should be manually locked and only unlocked and on ACS access mode during normal business hours.	It is not practical to key lock the rear door as there are only 2 keys, 1 held by the landlord and 1 by the GM Corporate Services. Increased camera coverage and bringing in-house swipe card access should mitigate the risk here.
19	Install an intercom at the second floor main entrance of number 10 or alternatively construct a reception area with the ability to isolate visitors if they are deemed hostile.	The foyer is intended to be used to isolate visitors before being greeted by staff. Recommend we direct all visitors to 6 Show Place to be vetted by security rather than install security and reception at 10 Show Place.
20	Secure the Lundia in a closed position at the end of the business day and attach a locking mechanism to the Lundia	The blinds provide good coverage from a confidentiality perspective to the Lundia. There are approximately 12 sensors across level 1, should the first sensor not pick up an intruder a number of the other should.
21	Secure protective grill or bars on the inside of the windows in the vicinity of the Lundia filing system.	As above, 20.
22	Improve quality of CCTV footage by replacing cameras for Atrium, Front Entrance and café exit.	Full review being undertaken with Sub 5 to upgrade existing cameras and increase the number of cameras on both sites.
23	Add camera down driveway between number 6 and number 10 covering drive and rubbish bin area.	As above, 22
24	Add camera to cover rear carpark	As above, 22
25	Add camera covering side door.	As above, 22
26	Construct a separate server room in number 10 Show place to house sensitive	Not practical to install room however enhancements will be investigated to secure IT

	IT equipment including the CCTV DVR. A room would also enable private reviewing and downloading of sensitive footage in the event of an incident once a monitor has been added to the system.	equipment. They are currently in a locked cabinet but enhancements could be made to the back of the cabinet.
27	Add external cameras for carpark and entrance security subject to landlord restrictions.	As above, 22
28	Add internal camera above main entrance door to capture facial images of people approaching the office door.	As above, 22
29	Install IDS at number 10 Show Pl.	In progress, phone line installed this week and alarm to be installed in the next couple of weeks.
30	Liaise with landlord to enhance lighting at back of rear carpark.	Agree
31	Security Incidents should be documented in the current HSE system so that they can be tracked and appropriate response measures can be initiated.	Agree
32	Security personnel should be trained in completing incident forms.	Agree
33	Cabinets with sensitive files should be locked at all times securing the documents within.	Not practical to lock files away, focus is on securing the building and those that enter to ensure confidentiality agreements in place.
34	Physical files, external electronic storage devices should be secured in locked cabinets.	As above
35	Laptops should be secured to the desk with security cables and logged off.	Not practical, laptops should be taken home as part of the ERT process.
36	All sensitive documents should be placed into the destruction bins provided and this should be enforced by management. Staff at all levels should be made aware of their responsibility to protect confidential information (Security awareness) both in the work place, at home and on location.	Agree and this has been reiterated in training sessions to all staff and will continue to be repeated.
37	Design a specific room for confidential meetings i.e. no electronic equipment (includes conferencing equipment, speakers etc), see through glass table top, bare walls, no additional furniture/fixtures. Ideally this room will be stand alone, central to the building, no windows, fitted with electronic access control and CCTV (Parallel layering).	Not practical, as mentioned in 33 above, the focus is on securing the building and those that enter to ensure confidentiality agreements in place.