1.0 Security risk analysis

1.1 Ten principles for risk analysis

1.2 When carrying out a risk analysis, ‘Reasonable’, ‘Realistic’ and ‘Risk Commensurate’ should be considered. Where funding is limited and risks are considered low, often a simple solution can be just as effective as a more complex one. e.g. intruder alarm or a simple window lock, which is a cheap and effective investment to prevent burglary? Consider the following when carrying out a risk analysis:

1.3 Target Removal

Permanent or temporary removal of the target (valuable item). This means ensuring the target is not visible from outside or is removed from public view. e.g. expensive computing equipment should be housed on an upper floor rather than ground floor, or away from external windows. Expensive or critical IT equipment might be housed off-site at purpose built IT premises.

1.4 Target Hardening

Make the target resistant to attack. Expensive IT equipment should be fitted within a steel enclosure or in a purpose made IT desk with security bolt. Where possible doors should be solid, within a strong frame and fitted with adequate locks. Window shutters or grilles should be considered for large areas.

1.5 Remove the Means to Commit the Crime

This is good housekeeping. Ensure that anything an offender may find useful to assist them, such as keys, tools, ladders etc are locked away and not left easily accessible. All scaffolding should be enclosed at ground level to prevent climbing.

1.6 Reduce the Payoff and Loss

What value is the item if stolen and resold externally? Consider the value of the loss if something was stolen. Property marking expensive items with the University postcode and the department name reduces the potential for resale and increases the chance of

the property being returned if found. Insurance cover is available but limited and the Policy excess may not cover the loss. Consider specific items insurance if critical.

1.7 Access Control

Where possible restrict access to a room, area, floor or building using access control. This can be video/entry phone system, a digital combination lock, or traditional key lock.

1.8 Visibility and Surveillance

Three methods of surveillance should be considered:

- Natural – the area is visible to other occupants or passers-by.
- Formal – using technology &/or people to monitor the area & deter offenders and having a procedure to deal with suspicious persons.

- Informal – encouraging employees to be vigilant.

1.9 Environmental Design

Putting in a range of security measures at the design or planning stage of a building or refurbishment, to reduce the risk of crime. Perimeter controls or surveillance methods should be considered.

1.10 Rule Setting

Local procedures as well as University Policy should be used. eg. Efficient evening locking up procedures for offices and IT rooms; local key issue and controls; a ‘communication tree’ for passing on important security information; exit procedure for staff who leave (to hand in ID card & keys and change access codes).

1.11 Increase the Chance of Being Caught

Any measure that slows down an offender or increases the chance of them being caught can be considered. The longer it takes to commit an offence the more vulnerable the offender feels. Some of the other principles cover this, such as target hardening, but also consider publicising security detection (CCTV warning signs) and any successes when criminals are caught.

1.12 Deflecting Offenders

Educational programmes, youth action teams, youth hobby groups, awareness programmes etc have all proved successful in deterring youngsters from offending and provide training and work experience. Can you offer any support to local groups?

2.0 SECURITY RISK ANALYSIS - SELF ASSESSMENT FORM

2.1 A security risk analysis should be carried out annually or whenever circumstances change which may affect security measures. This form is provided as an aid to self-assessment and does not necessarily cover every security circumstance or possibility.

	QUESTION	YES	NO	N/A	ACTION/ COMMENTS
A	**General:**				
1	Are your equipment inventories up to date? (These should list your valuable equipment with serial numbers, values, photos etc and can be produced to identify property subsequent to a theft, arson or vandalism)				
2	Have all the action points been carried out from your last security analysis?				
3	Have any crime or fire reduction measures been added since your last analysis				
4	Have there been any incidents of crime or suspicious activity in your area?				
5	If “yes” to previous question, have incident forms been completed and returned to Security				
6	Has damage from previous incidents been made good or improved to discourage re-offence?				
7	Has any guidance been sought on security measures from the Security Team?				

B	**Staff**				
1	Are new staff briefed on University Polices and any local Security Procedures?				
2	Are all staff trained in security awareness & to report suspicious activity, maintenance issues etc?				
3	Has a risk assessment been carried out on staff personal safety & any safety procedures published?				
4	Do staff know University emergency procedures?				
C	**Building Security**				
1	Are the premises in good repair?				
2	Are all doors locked when areas are vacated/not in use?				
3	Are windows closed when rooms/areas are not in use?				
4	Are windows blinds/ curtains closed at dusk? (ground floor in particular)				
5	Is good housekeeping in force to remove easy methods of access for offenders				
6	Is lighting effective (to deter intruders)				
7	Have intruder alarms been installed in high value or vulnerable areas				
8	Are intruder alarms working correctly and hardware maintained?				
9	Are intruder alarm users trained how to use the system				
10	Is the alarm set/unset each time the area is not in use?				
11	Are the alarm codes changed each time a member of staff leaves?				
12	Are IT theft prevention measures in place (High value items locked away out of sight)				
13	Are there secure storerooms or containers for securing attractive portable items such as laptops, AV equipment?				
D	**Keys:**				
1	Is there a proper system in place to control the issue of keys?				
2	Are lost or stolen keys reported to Security?				
3	Are locks changed when a key is lost?				
4	Is there an established procedure for locking up?				
E	**Cash**				
1	Does the department handle cash?				
2	If yes, are staff trained in cash handling procedures (see University Financial regulations)				
3	Is cash counted and stored out of sight?				
4	Are cash holding kept to a minimum?				
5	Is money stored in a safe and keys locked away?				
6	Is cash handling audited regularly?				
F	**Visitors**				
1	Are visitors collected from reception and escorted during their visit?				
2	Are unexpected or previously unknown visitors asked for identification?				
3	Are visitors/members of the public prevented from entering unauthorised areas?				
4	Do staff challenge strangers in unauthorised areas?				
G	**Security outside Office Hours**				
1	Do staff check that students & visitors have vacated the department at the end of the working day before locking up?				
2	Are staff who require out of hours access, trained in security procedures?				
H	**Contingency Planning**				
1	Do you notify the Security Manager when there are changes to out of hour contacts?				

2	Does the department have a local emergency or contingency plan to reduce or minimise disruption on activities after a serious incident?				
3	Are duplicate records & back-up copies of computer files maintained regularly and kept in a separate location?				
4	Is there a department communications tree for emergency contact? (including out of hours)				