

TEN POINT PLAN FOR PERSONAL ATTACK DEVICES

1) FILTERING

The ARC's are not in a position to pass only confirmed PA's to the police. The fact that someone does not answer the telephone does not confirm the activation is genuine as access to the telephone may be restricted, or that staff are too busy to answer it. In the event of the telephone being answered an operator is not always in a position to determine from what is (or is not) heard, if the activation is genuine.

However, the ARC's are in a position to attempt to filter unwanted false activations, with intervention in place false calls will be reduced.

2) WITHDRAWAL OF POLICE RESPONSE

The Intruder Alarm part of a system will be allowed to receive the current amount of false calls before withdrawal of response. Police response will be withdrawn to the PA part of the system after a maximum of 2 false calls in a rolling 12 month period.

Where a system loses response to a PA, the security company should liaise with the end user to see if the PA element is necessary. If it is not required it should be removed.

When a form of Intervention has been implemented, police response may be reinstated to PA's before the 3 month period. Any subsequent loss of response, after Intervention has been put in place, a system must achieve three consecutive months free of false calls supported by evidence from the security company.

3) PA DEVICES ON CIE OR ACE SHOULD BE SEGREGATED FROM THE MAIN KEYS, DEDICATED, DEFINED AND ARE 2 SEPARATE BUTTONS SYNCHRONISED PUSH.

4) PA DEVICES ON CIE OR ACE SHOULD BE ENGINEER PROGRAMMED ONLY (DEFAULT OFF)

The implementation of this action will be dependant on the programming ability of the CIE or ACE. Re-engineering may be needed and therefore a lead time will be required. This will stop the PA signal being transmitted during watchdog failures or if the CIE reverts to default programming due to power problems.

5) DURESS CODES SHOULD ONLY BE ALLOWED FOR BS 7042 OR BS EN 50131-1 GRADE 4 SYSTEMS

The logic of restricting duress codes to high security systems to ensure that the risk warrants the facility. Inadvertent use of the duress codes from the CIE lead to a significant abuse of Police manpower.

Individual applications for duress facility may be considered for Grade 3 systems if the following requirements are complied with:

1. In premises that require high security, has duress been identified as an essential requirement from the risk assessment?
2. Is the duress notified separately from the hold up alarm signal?
3. confirm that the means of unsetting is not option 6.4.5 DD243:2004

6) DURESS FACILITY SHOULD BE ENGINEER PROGRAMMED ONLY (DEFAULT OFF)

The implementation of this action will be dependant on the programming ability of the CIE or ACE. Re-engineering may be needed and therefore a lead time will be required. The purpose of this software change is to ensure that the duress facility is restricted to BS 7042 and EN 50131 grade 4 systems and not customer programmable. This will stop the duress signal being transmitted during watchdog failures or if the CIE reverts to default programming due to power problems.

APPENDIX T (continued)

7) **NO SINGLE ACTION 'SINGLE PUSH' PA DEVICES SHOULD BE ALLOWED**

Only 2 separate buttons with synchronised push systems should be allowed, as this would stop accidental activation by people 'bumping' against the PA. Although this has been standard in the industry for many years, systems may need to be upgraded to 'double push' PA devices in the event of losing police response

8) **NO TIME DELAY DEVICES ARE TO BE ALLOWED**

In these types of systems the PA is pressed once to start a timer. The occupier can then answer a door, check for intruders etc. If the PA is not pressed a second time, the timer will time out and the PA is sent. This type of arrangement is a recipe for false alarms and will need to be redesigned in the event of losing police response.

9) **PORTABLE PA DEVICES (WIRELESS DEVICES) SHOULD BE DEDICATED AND NOT INCORPORATE ANY OTHER FUNCTIONALITY AND SHOULD HAVE 2 SEPARATE BUTTONS, SYNCHRONISE PUSH TO ACTIVATE**

This requirement is to stop single button type PA's, e.g. care alarm type systems being used for PA's. Although this has been standard in the industry for many years, systems may need to be upgraded to 'double push' wireless devices in the event of losing police response.

10) **TRAINING / RE-TRAINING OF USERS**

The training or re-training of users should be incorporated into the maintenance. The user should also be made responsible for the training of their keyholder and this should be documented with the maintenance report.

Documentation should be provided to indicate when to use and when not to use a personal attack device. The keyholder should be made aware of the serious implications of misuse.