ANNEX E

TENANT RESTRICTED AREA SECURITY PLAN
MODEL OUTLINE

1. Programme Objective

2. Definitions

3. Tenant Restricted Area Boundary

3.1 General Description of security restricted area (e.g. enclosed single storey building; open area with public access to car park)

3.2 Description of the Tenant Restricted Area (TRA) and boundaries.

3.3 Reference to TRA boundary plans.

3.4 Location of TRA showing relation to lease boundary and rest of airport.

4. Physical Security

4.1 Perimeter fences ï plans of fence alignment to be included, with particular emphasis on interfaces with other fences and structures that vary in design to main fence or are the responsibility of other organizations.

4.2 Perimeter gates ï design and operation. Plans to be included.

4.3 Entry points ï design and operation. Plan to be included.

4.4 Security lighting ï make, model and operation. Plan to be included.

4.5 CCTV ï make, model and operation. Plans to be included.

4.6 Perimeter Intruder Detection System (PIDS) ï make, model and operation. Plans to be included where applicable.

4.7 Warning signs- design of sign with dimension, wording of warnings in the Filipino language and/or local dialect and English, locations and height of signs to be shown, relative to line of sight. Example of warning sign to be included. Consult the airport manager as he may have standard signage requirement to ensure uniform application throughout the airport.

4.8 Plans showing the locations of the items above. If possible, they should be incorporated on a comprehensive plan.

5. Security Operations

5.1 Hours of operation of TRA ï to include access and egress points and areas of the TRA, which will be effectively closed down and secured when not in operation.

5.2 Hours of duty of security guards.

5.3 Security staff and guard manning levels.

5.4 Command and control arrangement, including operational details of the control centre.

5.5 Testing of alarms.

5.6 Quality Control Measures

5.7 Screening (where applicable)

5.8 Interface with other Restricted Areas (where applicable).

6. Duties of TRA Security Staff

6.1 Security Manager (or person responsible for security matters).

6.2 Security Supervisors.

6.3 Guards ï specify for guards at each location / role (e.g. access control at main entrance; perimeter patrol; screening)

7. TRA Pass System

7.1 Types of passes, number of types and purpose, area and period of validity, format of pass with samples for each type.

7.2 Pass issue policy-who is entitled to a pass and under what circumstances (for each type of pass).

7.3 Pass application and issue procedure- details required for and format of application form with sample(s), supporting documents required, checks made to confirm details, person/ department responsible of processing application, person / department responsible for approving application, person / department responsible of issuing pass (for each type of pass).

7.4 Pass controls ï issue (initial), issue at shift start, collection at shift end, storage when not in use, verification of passôs validity during use (for each type of pass).

7.5 Condition of use ï display, transfer, reporting loss / damage.

7.6 Action and / or penalty in event of misuse / loss (for each type of pass).

7.7 Procedures for handling visitors if not included in the above.

8. Staff Training

8.1 Identity of person (by post) responsible for conducting security training to the TRA staff.

8.2 Details of including training ï security awareness (all staff) and security specific (staff with specific security responsibilities and duties).

8.3 Details of refresher training.

8.4 Copy of security training manual.

9. Security Contractor

9.1 Name and address of security contractor.

9.2 Description of services provided.

9.3 Copy of contractorôs requirement policy.

9.4 Copy of contractorôs training manual.

10. Security Equipment

10.1 Inventory and location of security equipment used under the TRA security programme.

10.2 Name and address of organisation maintaining security equipment.

10.3 Frequency of serviceability tests, records of results and details of remedial action.

11. Contingency Plans

11.1 Bomb threat.

11.2 Suspicious object found.

11.3 Fire.

11.4 Unauthorised access.

11.5 Access control system failure.

11.6 Injury to person on premises.

11.7 Electrical failure.

11.8 Communication failure ï telephones and / or radio.

11.9 System failure ï CCTV, alarms, Perimeter Intruder Direction System (PIDS).

Appendices

A. Company organisation chart.
B. Contact number of key personnel.
C. Engineering plans.