**SOP 10**

Security Officer Code of conduct

Main Enquiry Line:

Book On/Off:

Control Email:

Incidents Email:

**EMERGENCY NUMBERS**

**Landline:**

**Mobile:**

**Shift Managers Email:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_is operational 24 hours. Security Officers are required to report regularly to \_\_\_\_\_\_\_\_\_\_\_\_ and should do so at the times appointed. Failure to do so causes concern for your safety and can cause \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ to set Emergency Procedures into motion unnecessarily.

Security Officers must not leave the site without permission and without reporting to

\_\_\_\_\_\_\_\_\_\_\_\_\_. Sites must be manned at all times and if as a result of unforeseen

circumstances or sickness you have difficulty in getting to your place of work on

time, then you must advise \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ at the earliest possible opportunity to

ensure that they are able to provide suitable relief.

You SHOULD NOT UNDER ANY CIRCUMSTANCES leave the site until a

Replacement Security Officer arrives to relieve you.

Guard Base Location

It is the responsibility of the officer on duty to keep the Security Office & surrounding area clean and tidy. The Security office should be a central point for the collation of all security documents.

This includes assignment log books; copies of accident and incident reports and key log books

Monitoring of onsite equipment

Prior to the commencement to the contract the contract/site manager will produce an inventory of both client supplied and compass supplied equipment

The purpose is to provide a documented record of equipment supplied by the client. This can be useful in the event of damage or other disputes.

The Daily assignment log

This document is retained for the client’s information

The Dailey assignment log is to be updated throughout the security officer’s shift.

1. the security officer should complete the first section on commencement of duty and also record the fact that he /she has booked on duty with the communications centre entering ref number given
2. During the course of the shift, all activities and incidents must be recorded in chronological order, in either Black or Red ink giving all necessary details, e.g. names, vehicle registration number etc.
3. Ensure that accurate times are recorded for check calls and site patrols
4. Use the daily assignment log record any special requests or instructions from the client
5. Use the daily handover log to pass information to the in coming shifts

Dress, appearance and deportment:

Due to the high visibility of Security Personnel it is essential that their dress, deportment and appearance be of the highest standard.

Uniform, as supplied, should be worn at all times. Trousers should be pressed and if a belt is worn it should be black in colour. Short sleeved shirts to be worn and ironed should be fastened at all times. Ties should be cleaned and pressed. Black socks must be worn at all times whilst on duty.

At any one time all Officers on duty should be dressed the same.

Individual Officers must correct body odours, dirty fingernails, bad breath and unkempt hair.

Hair must be neat and tidy and in the case of male Officers, it should be worn above the collar and ears. Beards and moustaches may be worn but should be well trimmed and tidy. Female Officers must tie long hair back.

Male Officers who do not wear beards and/or moustaches should be clean-shaven at all times whilst on duty. Those wishing to grow beards and moustaches should ensure that the early days of growth are undertaken whilst off duty.

All Officers must not wear earrings , watches or jewelled rings to follow the NHS bare below elbow whilst on duty. Nose studs are prohibited for all uniformed Officers.

Sunglasses are not to be worn without a medical certificate. Where this is granted they should be of a plain frame and glass not fashioned or mirrored.

The most important factor is deportment, i.e. physical bearing and manner in which you behave.

**Do not** slouch about

**Do not** adopt an aggressive stance/confrontational manner

**Do not** walk about site with hands in pockets

**Do not** eat, drink, smoke, other than in designated rest areas, irrespective of whether on meal breaks or on/off duty

**Do**  act courteously at all times, even under provocation. Report any problems to your Supervisor who will ensure that they are dealt with through the correct channels

Conduct

Alcohol must not be consumed whilst on duty, nor immediately before coming on duty. No drugs or medication, whether prescribed or other wise, may be taken on duty without the authorisation from the Site Manager. Any member of staff SUSPECTED of being unfit through drink or drugs will be immediately suspended from duty.

Security Officers are expected to be alert at all times whilst on duty. Therefore radios, televisions, kettles, private study books or other reading material must not be brought onto site for use at security posts. Security Officers should not engage themselves in lengthy conversations, which may distract them from their duties.

ID cards & SIA Licence must be worn at all times & Displayed whilst on duty. Failure to have your SIA licence with you may result in you being removed from your assignment

Security Personnel should not load any software onto computers belonging to the client, nor should they alter the running of any programme without the authorisation from the Site Manager.

Parking for security personnel:

Security Personnel that drive to work and wish to park on site may park in the general parking areas, which are subject to spaces being available. The Security Manager may withdraw facilities for on-site parking at any time, without notice. Security Personnel must adhere to all parking regulations on site.

Private telephone calls

Security Personnel are not permitted to use company telephones for making or receiving private calls, use of mobile phones whilst on duty are prohibited.

In exceptional circumstances other arrangements can be made, i.e. privacy for a personal matter.

Should it be necessary for you to receive personal calls whilst on duty, you must notify COMMS in advance. It is accepted that this is possible should relatives/friends need to contact you in an emergency.

**REASONABLE REQUESTS**

All Medirest staff are to comply with any reasonable request from the client, as long as their health and Safety are not put at risk. If in any doubt contact the Site security manger or Contract director - Medirest.

**COMPUTER USE**

POLICY TITLE: COMPANY POLICY FOR COMPUTER USAGE INCLUDING E-MAIL

AND INTERNET ACCESS

Purpose of this Policy

The purpose of this policy is to ensure that all authorized personnel use computing

Facilities in an effective, efficient, ethical and lawful manner. Company computer

Hardware, software and data is for the exclusive use of the Company's business and

access to and use of such must be limited to employees of the Company, or advisors,

consultants and agents engaged by the Company.

Where Compass Group UK & Ireland employees have access to Client (where Compass

Group UK &Ireland has been contracted to provide services) company hardware,

software and data they remain bound by the terms of this policy. In addition, the

personal use of Client equipment is strictly prohibited without express written permission.

Where a Client policy on computer usage has been issued separately this takes

precedent, but only to such Client equipment and software. Any unauthorised access or

breach of this policy will be dealt with through the disciplinary procedure.

**Law**

Anyone using a computer system must comply with the Data Protection Act 1998 and all

copyright legislation on software or any other legislation, which may from time to time be

enacted. The storing, creating or passing on of text or graphics which could be regarded

as offensive on grounds of race, offensive, sex or disability is expressly forbidden.

Systems shall be routinely monitored for such content and appropriate actions taken as

outlined in the

**Disciplinary section of this code of conduct.**

Access to Computer Systems

* Use of a computer system is restricted to staff who have been given authority by their Manager.
* Passwords must not be communicated to an unauthorised person.
* Passwords should not be written down and left in visible areas, e.g. computer screens.
* Use of e-mail and access to the Internet is only allowed when authorised and in accordance with Company e-mail policy.

**Using a Computer System**

In order to prevent damage to a computer system by viruses or incompatible software:

* Only software authorised by Compass Group UK & Ireland IT department may be loaded on to your system. No other software should be loaded onto your system at any time.
* Use of Unlicensed software is illegal and any breach of the policy, in this area, will be regarded As Gross Misconduct, which could result in Summary Dismissal.

All software must be used within the terms of the software licence agreement. The IT

Department holds most licences and disks for Company software products. If this is not the Case then they should be kept in a secure place and produced for inspection if required. Software issued to staff must not be used on any other computer systems or modified Without prior authorisation. Data must not be extracted or copied from computer systems other than as authorised. The Company may use detection software to monitor compliance of this policy. Only equipment that has been authorised by the IT Department may be attached to Your System or the Compass Network.

Any abuse of this policy, which causes damage to computer equipment or incurs costs to the Company, may be deemed to be the responsibility of the employee.

Security For security reasons you should not divulge your logon ID or password

CONFIDENTIALITY

Security Officers must at all times during their employment on site and thereafter observe strict secrecy as to the affairs, dealings and concerns of the client. They must not, except in the proper course of his/her duties, disclose or assist in the disclosure of any trade secrets or other confidential information relating to the past, present or future operations and/or any business activities of the client or any subsidiaries.

###### Vehicle Logs

A record of all vehicles entering and leaving the site is to be kept on the log provided in the gatehouse. All details on the form must be completed.

**Telephones – THE BELOW IS AN EXAMPLE PROCEDURE**

The telephones should be answered, Good Morning, Good Afternoon or Good Evening, LTA then, 'how can I help you ' and in no less than 6 rings.

Example: Good morning LTA how can I help you.

If the officer is already engaged on a call, and the other line rings, you should politely ask the caller to hold, whilst the other line is answered, as the incoming call may be an emergency. Once the nature of the call is established, the second caller can be put on hold or asked to call back later.

All calls should be concluded as quickly as possible and personal calls should never be made from any of the phones on site.

Screening procedure for transferring emergency calls:

A switchboard operator receiving a request from a caller to either contact the emergency services or to be transferred to the emergency services must obtain the following:

* Name of the caller
* Extension number and department of the caller
* Nature and location of the incident
* Location of the caller

If the operator using the switchboard is satisfied that the caller is a genuine member of staff calling form an internal line, only then may they be transferred or the emergency services contacted. Security must be informed immediately by the operator so they can then respond to the incident and will also know to expect the emergency vehicles.

If the operator is not satisfied that the call is genuine or has been unable to trace the caller's details then the call must be transferred to security. Security will then deal with the caller.

An operator receiving a request for the emergency services from an external line should firstly be asked why the caller did not contact 999 directly. If the caller insists on being transferred to the emergency services then the switchboard operator must transfer the call to security.

An operator must never disconnect the caller and assume that they are making a hoax call. If in doubt, always transfer the call to security.

Operators becoming involved in genuine emergency calls may be required to complete an incident report for security records.

***CONFIDENTIALITY/DISCLOSURE OF INFORMATION***

Due to the nature of the client’s business, Security Officers are not permitted to discuss any information to which they obtain during the course of their duties. Outside agency or person officers are also prohibited from disclosing information gained.

# SUPERVISOR RESPONSIBILITES

* Responsible for the supervision of Security officers employed on the site and their standards of efficiency.
* Must be familiar with all Assignment Instructions, and other orders as may be issued from time to time.
* Ensure that all Security Officers are properly dressed, and fully aware of their duties and responsibilities.
* Responsible for the submission of site visits reports.
* Responsible for the tidiness of the Security Office.

Responsible for ensuring all tasks set have been carried out

|  |
| --- |
| SPECIFIC INSTRUCTIONS RELATING SOP10 |
| On the dates below I certify that I have received and fully understand the training in the correct use of the instructions specific to contract as specified by this procedure. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| OFFICERS NAME | PIN NUMBER | DATE TRAINING COMPLETE | OFFICER SIGNATURE | MANAGER SUPERVISOR NAME | MANAGER SUPERVISOR SIGNATURE |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |