

SECURITY POLICY – HRP001



General

Security is one of the most important issues affecting the Company's daily operation. This policy outlines the basis of security maintenance and control, and it is a requirement that the policy be complied with at all times. Each employee will be required to sign the appropriate acceptance sheet on receipt of his/her ID access card and door key as an acknowledgement of his/her responsibilities.

1. Building Access

- a. The front door will be locked at all times.
- b. It is anticipated that all access to and from the building will be via an access control biometric scanner linked to a security management system. Every employee will be provided with an access code on his/her first day of engagement. A front-door key will also be issued which is to be used by the last person leaving the building in the evening or weekend.
- c. Access to the building by non-Company personnel will be by invitation only and on the approval of a director. Under no circumstances will anyone be permitted to walk around the premises unaccompanied.
- d. **The last person leaving the building must:**
 - Check that all windows including men's and ladies' toilets are securely closed
 - Switch off all lights with the exception of the outside front door lights
 - Lower and close all blinds
 - Ensure the air conditioning is switched off (except computer room)
 - Ensure that the computer room door is closed and locked when appropriate
 - Activate the alarm
 - Lock the front door (using the key issued)

Should the last person leaving the building neglect to take the necessary security precautions (as set out above), and the alarm is activated as a result of his/her negligence, he/she will be liable for all resultant expenses incurred.

2. Alarm System

- a. The first member of staff entering, and the last member leaving, the building will be required to arm or disarm the alarm system by punching in the appropriate code on the keypad next to the front door.
- b. The code, and any changes to it, will be communicated to all staff.
- c. Should the code be incorrectly entered when accessing the building, or the alarm activated at any time whilst the building is occupied, the contracted security company will phone the Company's switchboard and request the password and the name of a staff member on site. If the incorrect password is given, an armed response unit will be deployed to the building. The password may change from time to time and the new one will be communicated when necessary.
- d. It is incumbent on all staff to make themselves aware of all codes and passwords at all times and under no circumstances should these be passed on to anyone other than the Company's staff.
- e. External contractors will not be allowed to work unattended in the building nor be given any security information.
- f. Management will carry out random security checks to verify system functionality and the security company's service levels.

Description:	Security Policy	Policy Number: HRP001
Department:	Human Resources	
Responsibility by:	All / Facilities	
Last Saved:	22/7/2019	
	HRSimplified - Security Policy	Page 1 of 2
	HRP001	

The contents of this document are strictly confidential. The contents are for the internal use HRSimplified Online Customers staff and/or persons as authorised by management.

SECURITY POLICY – HRP001



3. Keys

- a. A list of access key holders will be maintained for purposes of control and monitoring. No keys may be duplicated except with the approval of management.
- b. Any loss of keys should be reported to management immediately (irrespective of time of loss) whereupon the appropriate action will be taken.

4. After-Hours Contacts

- a. A list of emergency after-hours contact names and numbers will be maintained and given to the security company

5. Shredding

- a. All sensitive information or documents should be shredded prior to disposal.

6. Copyrights

- a. Under no circumstances will any copyrighted material be used illegally. Any picture, video clip, text and other electronic form of data, downloaded from the Internet or received via any form of networking, should be regarded as protected by copyrights unless it specifically states otherwise.
- b. Failure to adhere to a) above will result in disciplinary action.

7. Working After-Hours

Employees are allowed to work after hours till **18h00** during winter (May, June, July, August, September) and **19h00** during summer (Oct, Nov, Dec, Jan, Feb, Mar, Apr).

The only time employees are allowed to work later than the times stipulated above are in the instances where client change requests need to be worked on, on provision that all client change requests need to be approved by a Manager and the Client. In such instances there should be more than one employee on site.

8. Non compliance

Failure to comply with this policy, which will be perceived as negligence on the part of the employee, will result in disciplinary action being taken against the relevant employee.

Description:	Security Policy	Policy Number: HRP001
Department:	Human Resources	
Responsibility by:	All / Facilities	
Last Saved:	22/7/2019	
	HRSimplified - Security Policy	Page 2 of 2
	HRP001	

The contents of this document are strictly confidential. The contents are for the internal use HRSimplified Online Customers staff and/or persons as authorised by management.