

Administration	Buildings & Capital Assets	Board Approved Date:	21-02-24
Policy	Security	Revision Date:	N/A
Policy No.	20-092	Internally Approved Date:	20-09-26
References	Privacy and Confidentiality Policy Key Control Policy Common Room Rental Policy Video Surveillance Policy Parking Policy Personnel Policy Workplace Violence and Harassment Policy Dispute Resolution Policy		
Forms	Incident Report Form		

1. Policy statement

DRNPHC is committed to the provision of safe and secure housing communities. Such communities are created through proactive, prevention-oriented activities as well as timely and active response to crime as it is reported.

2. Purpose

It is the purpose of this policy to outline security features DRNPHC has implemented in order to support the safety and security of tenants, their guests, DRNPHC staff, volunteers, and members of the public and to safeguard the property of DRNPHC.

3. Scope

This policy applies to the board of directors, all staff and volunteers of DRNPHC in the performance of their duties, tenants and contractors.

4. Definitions

Designated Staff

The staff person(s) or department who has been designated to complete a particular action or requirement.

Security Personnel

Security patrol officers from a security company who have been hired by the non-profit to provide security duties or protection services.

Sensitive Data

Any financial, corporate, or legal information related to the non-profit, its activities, and its interests, including the personal information collected by the non-profit from applicants, rent-geared-to-income and market rent tenants, staff, board members, volunteers, contractors, community support services, and others.

5. Procedure

a) Safety Audit

Staff will ensure that safety audits are conducted on the properties on an annual basis.

Any new safety-related concerns will be forwarded to a supervisor or manager for further investigation, analysis and appropriate follow-up.

b) Security measures

Video surveillance

DRNPHC has often installed video surveillance in the building/on the property to protect public safety, corporate assets and property, including detecting and deterring criminal activity and vandalism. Refer to the *Video Surveillance Policy* for procedures governing its use and the protection of the personal information collected.

Key control

DRNPHC has implemented a combination of locking systems including keys and fob/access cards to secure the building, individual units, common areas and services rooms. Refer to the Key Control Policy for procedures governing their management and distribution.

Securing the Main Office

DRNPHC office staff will ensure that the following anti-intrusion measures are implemented to prevent unauthorized access to the office and confidential information:

- staff where appropriate, will have access only to the office and to confidential information if it is required in the performance of their duties
- confidential documents are to remain under lock and key and kept in secured filing cabinets when not in use and out of sight when staff are away from their desk, or work space
- confidential documents will be removed from the office only when required (e.g., for Landlord and Tenant Board hearings) and may never be left unattended, including in locked vehicles
- petty cash, business credit cards and passwords, will be locked in DRNPHC's fireproof safe when staff are away from their desk and after office hours. Business credit cards assigned to specific employees are placed in that employees care for safe keeping.
- doors and windows giving access to the office will be locked after normal working hours or when staff temporarily leave the office
- a security alarm will be installed to protect the office from unauthorized entry
- the security alarm will be set when leaving the office at the end of each business day
- the combination for the safe, passwords and the code to the alarm will be issued to full-time employees only if the employee's job responsibility requires such assignment as approved by the CEO. The code to the safe (if programmable) and computer passwords will be changed on a regular basis, particularly when there is a change in staff

Securing Other Office Spaces

DRNPHC office staff will ensure that the following anti-intrusion measures are implemented to prevent unauthorized access to all offices and confidential information:

- staff where appropriate, will have access only to the office and to confidential information if it is required in the performance of their duties

ADMINISTRATIVE POLICY - BUILDINGS

- confidential documents are to remain under lock and key and kept in secured filing cabinets when not in use and out of sight when staff are away from their desk, or work space
- confidential documents will be removed from the office only when required (e.g., for Landlord and Tenant Board hearings) and may never be left unattended, including in locked vehicles
- doors and windows giving access to the office will be locked after normal working hours or when staff temporarily leave the office

Electronic data and storage devices

The designated staff will ensure the following:

- all computers including offsite back-ups are password protected, loaded with anti-virus software and firewalled as per the *Privacy and Confidentiality Policy*
- if the DRNPHC hosts a website, it must be secured from cyber attacks
- computers/server will be backed up daily
- back-up copies of computer data will be stored off-site and in a secure location
- Corporate files are protected by Active Directory permissions that limit access to information based on staff profile.
- Staff are not to share usernames and passwords that could provide unauthorized access to sensitive information.
- all inactive documents and files will be stored in a secure storage facility at Wood Farm Manor, 1525 Nichol Avenue, Whitby, with limited access until such time as they are ready for disposal according to the *Records Management Policy*
- Physical files and/or documents containing confidential information will be disposed through a secure document disposal contract with an approved vendor.
- when disposing of old computer equipment, after deleting files using third party software from the hard drive to make the device unreadable, will be destroyed.

Maintaining a safe workplace

DRNPHC, as an employer, will take all reasonable precautions to protect its staff and volunteers from experiencing workplace violence, harassment, or domestic violence in the workplace in accordance with the *Occupational Health and Safety Act*. This includes working with staff members on a personal safety plan, if a risk to their safety has been identified.

The staff are encouraged to:

- report any threat or occurrence of risk in the workplace according to the *Workplace Violence and Harassment Policy*
- to keep supervisors and co-workers informed of their whereabouts in and around the building
- work in pairs when necessary (e.g., unit inspections)
- use the cell phone provided by DRNPHC to keep in contact with the office

Where a risk to a staff member's safety has been identified, the following additional security measures will be considered:

- installing a buzzer system in the office for staff working alone,
- relocating an employee's workspace to a more secure area

- screening phone calls and removing their name from any internal telephone directories
- if necessary, working with police to enforce restraining orders or develop safety plans

Security Services

In the absence of an on-site superintendent or in extenuating circumstances DRNPHC may require security of the building and grounds.

If DRNPHC has hired a security company, the security company will:

- provide twenty-four hour (or other hours as assigned) per day patrolling, with particular emphasis during periods that are not considered normal working hours
- investigate occurrences related to the protection of tenants and their guests and the property of DRNPHC
- call emergency services as appropriate
- will wear approved uniforms and will carry identification to provide clear recognition while on duty
- will ensure common room and laundry room doors and all exterior doors are locked while conducting regular patrol rounds
- Patrol rounds will be conducted on a random basis in order to avoid predictability
- follow directions regarding any other duties as assigned

Reporting

All occurrences reported to the Security Services must be recorded on an *Incident Report Summary* and reported promptly to the property manager or on-call person for review and follow-up and if necessary further investigation according to the *Dispute Resolution Policy*.

Enforcement

Protection services personnel are authorized to enforce at their discretion the *Common Facilities Policy* by terminating a function and asking guests to leave the premises if the event is found to be disturbing their neighbours or to be in contravention of the policy. They are encouraged to call police if they are at all concerned for their own safety or that of tenants and their guests.

Privacy

The security contractors will be required to sign a confidentiality agreement as per the Privacy and Confidentiality Policy and must not disclose any confidential information that is learned through the commission of duties other than to DRNPHC (as appropriate).

End.