PHYSICAL SECURITY

Policy and Procedures

Effective: November 2023

To be reviewed: November 2026

To help the public service
spend wisely

TABLE OF CONTENTS

CONTENTS

INTRODUCTION

1. The Office of the Auditor General (the "OAG" or "Office") is committed to maintaining a secure environment for its employees, clients, visitors, and assets. This policy outlines the guidelines and procedures to ensure the physical security of our office premises, equipment, and employees.

SCOPE

2. This policy applies to all employees, contractors, visitors, and individuals who access the OAG's office facilities.

POLICY OBJECTIVE

3. This policy aims to outline the measures taken to ensure the safety of employees and visitors to the office. We aim to implement security measures to control and manage access to our office to prevent unauthorised access, ensuring that only authorized individuals can enter. These measures will assist us in protecting our office assets, including equipment, data, confidential documents, and sensitive materials, from theft, damage, and unauthorized removal. The safety of our staff is our top priority, and we aim to create a safe environment for employees, and visitors, by minimising risks related to emergencies and accidents.

POLICY GUIDELINES

4. The Office has installed a security access system; the Corporate Services Manager and Deputy Auditor General – Corporate Services have administrative rights to grant access to authorised personnel. Access to the office premises is controlled through security key fobs, where access permissions give access to all areas.

5. All visitors are required to ring the intercom at the door, and the Administrative staff or any other staff are to attend to the visitor at the office lobby. An OAG employee must escort visitors at all times.

6. Exterior doors to the office and building will remain locked during non-business hours, and staff will require key fobs to gain access. The landlord controls the access to the building, and any issues with access to the building should be reported to the Corporate Services Manager or Administrative Assistant, who will inform the landlord.

7. Adequate lighting will be maintained around the office premises, including entrances and parking areas. Individuals parking in the overflow lot across the street are asked to take extra precautions when leaving late. We recommend that you park your vehicle in the main parking lot after hours.

8. In the event of an emergency, the OAG Business Continuity Plan sets out the emergency evacuation plan. The OAG's Fire Marshalls are the Corporate Management Team ('CMT") who will provide staff with instructions in the event the fire alarm is activated. However, in any event, you should leave your belongings and proceed to the nearest fire escape or staircase. CMT members will conduct a roll call once everyone has evacuated the building ensuring all staff are accounted for and safe. Under no circumstances should anyone use the elevators. Fire extinguishers, first aid kits, and emergency exits will be clearly marked and easily accessible. The landlord has not erected muster locations. However, OAG employees should muster away from the building at the most easterly side of Anderson Square parking lot which is close to the road by the Piccadilly Building.

9. Equipment and data security is a priority; therefore, all laptops and other portable equipment should not be left unattended in common areas. Additionally, if staff take OAG equipment out of the office on official business this should not be left unattended and should be stored securely. Access to the equipment should not be shared, nor should it be used by non-OAG Staff, except CIG Computer Services Department staff. Valuable equipment will be stored securely when not in use.

10. All employees should practice clearing their desks of sensitive information and lock drawers when leaving the office at the end of the working day. Staff should also 'lock' their computers when they are away from their workstations.

11. Personal data and confidential documents should be securely stored. When personal hard copies of the documents are no longer needed these should be shredded. Please note that if the information is the only record we have, ensure that it is stored properly. We are required to comply with the *National Archive and Public Records Act*, which makes it illegal to destroy public records without the National Archive's approval.

12. Employees must report any security incidents, breaches, or suspicious activities to the Deputy Auditor General – Corporate Services and/or the Corporate Services as soon as possible after the incident.

POLICY REVIEW

13. This policy will be reviewed every three years to ensure its effectiveness and alignment with changing security needs.