Secretariat for Administration and Finance

Organization of American States

ADMINISTRATIVE MEMORANDUM No. 126

SUBJECT: ACCESS CONTROL POLICY FOR OAS HEADQUARTERS BUILDINGS

CONSIDERING,

All staff members and other personnel of the General Secretariat have a vested interest in the continued security of OAS facilities, including the security of meetings such as OAS General Assembly when held at OAS Headquarters, as well as the security of daily access to OAS facilities by staff members, other OAS personnel, and individuals from outside the Organization;

The Security Section of the GS/OAS is charged with creating an integral access control policy in order to protect the property, personnel, tenants and guests of the Organization at the Headquarters facilities of the Organization. One of the primary ways of protecting these elements of the OAS is through the issuance of identification cards, access passes, and the implementation of building access procedures. Therefore, there is a need for an Access Control Policy to apply to OAS Headquarters facilities, and to any other OAS facility as determined by the General Secretariat; and

All individuals who intend to access the facilities of the OAS should be made aware of the protocols in place for secure access to said facilities.

THE DECISION:

To institute the following Access Control Policy as set forth in Attachment A.

Peter A. Quilter
Secretary for Administration and Finance

Original: English
July 7, 2015

Attachment A

Access Control Policy for OAS Headquarters Buildings

1. Purpose

The Department of General Services/Security Section of the General Secretariat of the Organization of American States (GS/OAS) is charged with creating an integral access control policy in order to protect the property, personnel, tenants and guests of the Organization at the Headquarters facilities of the Organization. One of the primary ways of protecting these elements of the OAS is through the issuance of identification cards, access passes, and the implementation of building access procedures. This Access Control Policy shall apply to OAS Headquarters facilities, and to any other OAS facility as determined by GS/OAS.

2. General Policy Statement

It is the policy of GS/OAS that all people entering any OAS Headquarters facility, including parking facilities, shall pass through a security access control prior to entry. Individuals subject to security access upon entry shall include:

1) All staff members, contractors, volunteers, interns and other personnel of GS/OAS;

2) All government employees, contractors, and other personnel from OAS Member State Governments, including personnel of Permanent Missions and Observer Missions to the OAS;

3) All individuals invited or granted credentials by OAS to participate at OAS meetings, the OAS General Assembly, the OAS Permanent Council meetings, meetings of the specialized organs of the OAS, or other official meetings of the OAS or its organs;

4) All tenants and licensees of OAS property, and their invitees and guests; and

5) All visitors to the OAS.

All individuals shall pass through some form of security access control prior to entering any OAS facility, to include parking areas. All persons who wish to enter any OAS facility must be identified either by presenting an official OAS identification card, or by presenting Government issued identification. Visitors to OAS facilities will be required to participate in security screening procedures prior to entry. The below sections of this policy will provide a detailed description of the specific requirements for accessing OAS facilities.

3. Employee Use of Identifications

All GS/OAS employees, government personnel from Missions to the OAS, tenants, and any other holders of an official OAS-issued ID must present this identification to a security officer for visual examination (or at the proximity card reader at parking lots and Administration building) in order to gain entry to an OAS building. The OAS ID shall be worn in a visible manner while inside OAS properties.

If the OAS ID is expired or if the person fails to produce his/her ID, upon attempting to enter the facility, the individuals shall not be allowed to pass the security desk until he/she has shown an official identification, the officer has confirmed his/her current rights to access the OAS, and issued a one day temporary pass to the person (to be worn by the employee in a visible manner). OAS identifications may only be used and presented by the person who is pictured on the identification.

Limited Exceptions: In consultation with the Department of General Services/Security Section, there shall be exceptions for Ambassadors, pre-identified Heads of State/Prime Ministers, the OAS Secretary General, the OAS Assistant Secretary General, and Chief of Staff of the Secretary General. Any or all exceptions to this policy require prior coordination with the Security Section. The Secretary General may designate any specific exception, and such exception must be on file with the Security Section in order to be effective.

4. Participants at OAS Meetings, other official meetings of the Organization at its Headquarters, and Additional Protocols for OAS General Assembly

All individuals participating at official meetings of the OAS, including meetings of its Permanent Council, meetings of the specialized organs of the OAS, and other official meetings of the OAS shall require identification and presentation to the Security Desk prior to entry to any OAS Headquarters Facility as indicated above at item 3; however, additional protocols may be necessary for entry as indicated by the Security Section.

Additional Protocol for OAS General Assembly, and other Meetings:

As an added measure of security at the OAS General Assembly, all individuals including GS/OAS employees and all others, shall be required to obtain Official Credentials granted for the sole purpose of entry into the General Assembly meeting place. The GS/OAS shall grant an Official Credential specially and individually to persons officially designated and accepted to participate at the OAS General Assembly. Said Official Credentials are special to the individuals to whom they are granted, are non-transferrable, and shall not be altered in any way, as discussed below in section 7 Sanctions For Violation. The same or similar Official Credential protocol shall be executed for Special OAS General Assemblies, Meetings of Consultation of Ministers of Foreign Affairs, and as needed.

The Official Residence is not open to the public, and the Security Section shall govern access to that Headquarters Facility under separate cover of a special protocol intended for that purpose.

5. Visitor Procedures

All visitors to the OAS Headquarters facilities of the Main Building, General Services Building, Administration Building, and the Casita of the Museum of the Americas, will be required to check in at a security desk, provide government identification, and may be subject to passing through a metal detector and a bag check (required at Main Building and GSB). All visitors must have a verified appointment with an employee or tenant of the OAS, and must be escorted to and from the lobby by the hosting employee or his/her designee. No visitor will be allowed to pass the security desk until an employee escort has arrived at the lobby. Visitors will wear the issued visitor pass in a visible manner while in OAS properties and must

return the pass to a security officer prior to leaving the building. The Chief of Security shall have the authority to reject or remove any visitor to the OAS.

Tourists: Tourists visiting the Main Building during regular business hours shall be duly screened by security, which may include passing through a metal detector and a bag check (both apply at the Main Building and bag check only at the Museum of the Americas). Tourists shall not be allowed in the facility after or before regular work hours of 9 a.m. and 5 p.m. Monday through Friday, except holidays. This tourist policy shall also apply to the Museum of the Americas.

Guests at rented OAS Special Events: Guests who arrive for contracted Special Events (i.e. paid events where OAS facilities are rented by outside parties pursuant to the Special Events Policy, Administrative Memorandum 68 and its current revision) shall adhere to the security policy stated in Administrative Memorandum 68. This Access Control Policy includes identification of all guests by the party renting the OAS facility, the obligation to contract for additional security personnel, and the use of metal detectors. This Access Control Policy shall compliment and fortify the security protocol for Special Events.

6. Caterers and Service Providers

All caterers and service providers for special events and building maintenance at the OAS must be pre-identified on a list, which shall be given to the relevant security desk by the associated OAS staff person or tenant. All caterers and service providers must present an official government ID prior to gaining access to an OAS facility and may be subject to passing through the metal detector or a bag check. Caterers and service providers shall be escorted to and from their pre-determined work area by the relevant OAS staff person or tenant.

7. Sanctions for Violation

Flagrant, intentional, or repeated violations of this Access Control Policy shall subject the violator to either the internal disciplinary norms of the Organization, as well as arrest and detention by U.S. law enforcement -- or both -- depending on the severity of the Access Control Policy violation.

For those individuals who are not subject to the internal norms of the OAS (i.e. individuals who are neither staff nor contractors nor other personnel of the GS/OAS), any flagrant violation of Access Control Policy shall be considered an unauthorized and unlawful entry onto the premises of the OAS, which shall prompt the immediate recourse to U.S. Federal and local law enforcement. Violators shall not be granted any access to legal assistance by the GS/OAS or any of its authorities while they are detained by law enforcement. Moreover, GS/OAS shall within its discretion pursue criminal trespass charges against all flagrant violators of this Access Control Policy. Violators shall bear all costs and legal consequences of the criminal defense and adjudication process in the territory of the United States.

For the purposes of this Access Control Policy, a Flagrant Violation shall include, among others, the alteration or transfer to any third party of any identification, including the alteration or transfer of the Official Credential issued as an additional protocol for the OAS General Assembly. Flagrant violations shall

also include allowing any third party access to GS/OAS facilities that is not authorized to be present at OAS facilities.

For those individuals subject to the OAS Staff Rules, flagrant violations shall be considered serious misconduct under the Staff Rules. Such a determination shall not preclude other discipline as contemplated under the Staff Rules.

For contractors and licensees, flagrant violations shall be considered grounds for termination of contract for cause.

8. Publication of Access Control Policy

GS/OAS shall publish this Access Control Policy. In addition, all managers of all OAS organs and dependencies holding meetings at OAS facilities shall be responsible for communicating this Access Control Policy to all individuals prior to their arrival at OAS facilities. GS/OAS managers' failure to communicate this Access Control Policy may be considered a repeated violation of this policy, and subject the manager to discipline under the Staff Rules.

Notwithstanding the foregoing, any determination of flagrant violations of this policy as discussed above shall not be mitigated by the fact that any violating individual was unaware of this Access Control Policy.

The Security Section may revise, update, and supplement this Access Control Policy as necessary.