MIA Road, NAIA Complex
Pasay City, Philippines 1300

www.miaa.gov.ph
(632) 877.1109

MANILA
INTERNATIONAL
AIRPORT
AUTHORITY

APR 20 2022

MEMORANDUM CIRCULAR NO. 11
Series of 2022

SUBJECT: PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

GENERAL

1. The Manila International Airport Authority (MIAA) is mandated to provide safe, efficient, and reliable airport facilities for international and domestic travel. The Authority is also responsible for, and committed to, the confidentiality, integrity, and availability of Information Technology (IT) networks, systems, and applications within the scope of its authority.

2. As a policy of the State, the Republic Act 10173 or Data Privacy Act of 2012 protects the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth. It also recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.

3. ISO 27001 Annex A.11 addresses the Organization's physical and environmental security. It is to prevent unauthorised physical access, damage or interference to the organisation's premises or the sensitive data held therein.

PURPOSE AND SCOPE

4. To protect the confidentiality and integrity of information technology and data as well as the safety of personnel, the Authority and its stakeholders must ensure that physical and environmental security controls are established to promote the security posture of MIAA.

5. This policy applies to all MIAA and stakeholders officers, directors, employees, agents, affiliates, contractors, consultants, advisors, service providers and other government agencies that are involved in the physical or environmental security protection process. It is the responsibility of all the above to familiarize themselves with this policy and ensure adequate compliance with it.

DEFINITION OF TERMS

6. For the purpose of this circular, the following terms shall be construed to mean:

a. **Airport Complex** – refers to the areas of MIAA Administrative Building, NAIA Terminals 1, 2 3, 4 and International Cargo Terminal.

b. **Fire Suppression Device** – system used to extinguish or control a fire.

c. **Organization** – refers to the Manila International Airport Authority and all its stakeholders.

d. **Output Device** – any peripheral that received data from a computer, usually for display, projection or physical reproduction.

e. **Physical and Environmental Hazards** – an act of terrorism, vandalism, unauthorized entry, flooding, fire, earthquake, hurricanes, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic interference.

f. **Security Operation Center** – is a hub for centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

STATEMENT OF POLICY

7. Physical access to information technology processing equipment, media storage areas, and media storage devices and supporting infrastructure (communications, power, and environmental) must be controlled to prevent, detect, and minimize the effects of unauthorized or unintended access to these areas.

POLICY GUIDELINES

8. Physical and Access controls within Airport Complex will follow the requirements outlined below:

a. Policy and Standards
The organization will develop, document, and disseminate formal physical and environmental protection standards that set criteria for: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

b. Physical Access Authorization and Maintenance
The organization will develop and maintain a list of personnel authorized to enter controlled-access facilities where information systems reside and identify those areas in a facility which are designated publicly accessible.

The organization will manage the list and all associated logs of access, including:

i. Track names and status of all who have been issued authorized credentials for facility access
ii. Identify and implement regulatory and policy log-retention requirements
iii. Regularly audit the detailed access log(s) of facilities
iv. Regularly review the access list, and promptly remove individuals from the facility access list when access is no longer required

c. Physical Access Control
   i. The organization will enforce physical access controls for all physical access points to the controlled facility. This includes:
   ii. The organization will verify individual authorization before granting access.
   iii. The organization will control entry to the facility using physical access devices and/or guards
   iv. The organization will maintain physical access audit logs
   v. The organization will implement additional controls, to include

      - Require two level approval of the needed access for personnel(s) within the systems.
      - Escort visitor and monitor visitor activity
      - Secure keys, combinations, and other physical access devices
      - Inventory physical access devices annually and conduct routine maintenance checks to verify that devices are functioning properly
      - Change combinations and keys annually or when keys are lost, combinations are compromised, or when individuals are transferred or terminated
      - Deactivate or revoke user access credentials upon transfer or termination

d. Access Control for Transmission Medium
   The organization will control physical access to system distribution and transmission lines, for example: lock wiring closets; disconnecting or locking spare network jacks; or protecting cabling by conduit or cable trays.

e. Access Control for Output Devices
   The organization will control physical access to information system output devices to prevent unauthorized individuals from obtaining output.

f. Monitoring Physical Access
   i. The organization will monitor physical access to the controlled facility to detect and respond to physical security incidents.
   ii. The organization will review physical access logs every 30 days and upon the occurrence of any known physical-access violation.
   iii. The organization will coordinate the results of the reviews with the defined incident response team (e.g., the Security Operations Center).

g. Access Records
   The organization will maintain visitor access logs for controlled facilities according to the retention guidelines and ensure the logs are reviewed regularly.

9. Environmental Control within Airport Complex will follow the requirements outlined below:

a. Power Equipment and Power Cabling.
   The organization will protect power equipment and power cabling for information assets from damage and destruction

b. Emergency Shutoff
   i. The organization will provide the capability to shut off power to information systems in a facility or individual system components in emergency situations.

ii. The organization will place shut-off switches or devices in a defined location to facilitate safe and easy access for personnel while protecting emergency power shutoff capability from unauthorized activation

c. Emergency Power
The organization will provide a short-term uninterruptible power supply (UPS) to utilize if the primary power source fails.

d. Emergency Lighting
i. The organization will employ and maintain automatic emergency lighting for the information systems that activate in the event of a power outage or disruption.
ii. Lighting will be provided for emergency exits and evacuation routes within the facility.

e. Fire Protection
The organization will employ and maintain fire suppression and detection devices or systems for the information systems that are supported by an independent energy source such as UPS.

f. Temperature and Humidity Controls
The organization will maintain temperature and humidity levels at operational levels within the facility where the information systems reside, and continuously monitor temperature and humidity levels.

g. Water Damage Protection
The organization will protect information systems from damage resulting from water leakage by providing primary shutoff or isolation valves that are accessible, working properly, and known to key personnel.

h. Delivery and Removal
The organization will authorize, monitor, and control equipment deliveries, moves, and removals from the facility, and maintain records of those moves.

i. Alternate Worksite
An alternate work sites, the organization will employ IT controls, such as logical and physical access controls, as necessary.

j. Location of Information Asset Components
The organization will position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

k. Annual Testing
The organization will test environmental systems and emergency sources at least annually to ensure continuous protection is in place.

PENALTY CLAUSE

10. The Authority identifies the minimum requirements necessary to comply with the information security standards and guidelines. Any attempt to disable physical and environmental security, such as disabling fire alarms, access entry system, or

permitting unauthorized personnel to "piggyback" and gain unauthorized entry into a controlled facility, will be considered a security violation and subject to investigation and possible disciplinary action which may include written notice, suspension, cancellation of pass, termination, and possible criminal and/or civil penalties.

SUPERSESSION CLAUSE

11. All orders, memoranda and/or other MIAA issuances inconsistent herewith are hereby amended and superseded accordingly.

EFFECTIVITY

12. This MC shall take effect immediately.

For strict compliance.

EDDIE V. MONREAL
General Manager

MCAO-CDL9FW