12-6

شركة شبكة الخدمات الآلية
Automated Services Network Co.

Physical Security Policy

Version: 1.7

Approved Date: 3-08-2026

Approved by:

Sabah K. Al-Ghunaim

Chairman

شركة شبكة الخدمات الآلية
Automated Services Network Co.

Contents

Policy Statement 3

Purpose 3

Scope 3

Employees 3

Documentation 3

Document Control 3

Records 4

Distribution and Maintenance 4

Privacy 4

Responsibility 4

Policy 4

Enforcement 6

Review and Revision 6

Acknowledgment of Physical Security Policy 6

Signature 6

Policy Statement

To meet the company business objectives and ensure continuity of its operations, Automated Services Network Company shall adopt and follow well-defined and time-tested plans and procedures, to ensure the physical security of all information assets and human assets. Physical security is an essential part of a security plan. It forms the basis for all other security efforts, including personnel and information security. A balanced security program must include a solid physical security foundation. A solid physical security foundation protects and preserves information, physical assets, and human assets.

Purpose

The purpose of the Physical Security Policy is to:

- Establish the rules for granting control, monitoring, and removal of physical access to office premises.
- To identify sensitive areas within the organization; and
- To define and restrict access to the same.

Scope

Employees

This applies to all employees, contractual employees, trainees, privileged customers, and all other visitors.

Documentation

The Physical Security Policy documentation shall consist of Physical Security Policy and any related procedures & guidelines.

Document Control

The Physical Security Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purposes.

Records

Records being generated as part of the Physical Security Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

Distribution and Maintenance

The Physical Security Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the Physical Security Policy document will be with the CISO and system administrators.

Privacy

The Physical Security Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

Responsibility

The General Manager is responsible for the proper implementation of the Physical Security Policy.

Policy

Following are the policies defined for maintaining Physical Security:

1. Physical access to the company shall completely be controlled by biometric access control devices.

2. Access to the company shall be restricted only to employees. Guests and visitors will be allowed to enter to reception area only and shall be escorted by an employee.

3. Physical access to the server room shall completely be controlled by biometric access control device and servers shall be kept in the server racks under lock and key.

4. Access to the servers shall be restricted only to designated Systems and Operations Personnel. Besides them, if any other person wants to work on the servers from the development area, then he/she shall be able to connect to the servers only through Remote Desktop Connection with a Restricted User Account.

5. Critical backup media shall be kept in a fireproof off-site location in a vault.

6. A list of personnel with authorized access to the facilities where information systems reside shall be maintained with appropriate authorization credentials. The access list and authorization credentials shall be reviewed and approved by General Manager periodically. The current List includes below personnel:

    a. Network Administrators
    b. Technical Manager
    c. General Manager

7. All physical access points (including designated entry/exit points) to the facilities where information systems reside shall be controlled and access shall be granted to individuals after verification of access authorization.

8. Physical access to the information systems shall be monitored to detect and respond to physical security incidents.

9. Physical protection against damage from fire, flood, civil unrest, and other forms of natural and man-made disasters shall be designed and applied.

10. Physical protection and guidelines for working in the areas where information systems reside shall be designed and applied.

11. Information systems and their components shall be positioned within the facility to minimize risks from physical and environmental hazards and opportunities for unauthorized access.

12. Information systems shall be protected from power failure and other disruptions caused by a failure in supporting utilities.

13. Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

14. The real-time physical intrusion alarm and surveillance equipment shall be monitored.

15. Physical access control to information systems shall be independent of the physical access control to the facility. This control can be applicable to server rooms or information systems with a higher impact level than that of most of the facility.

16. Physical access to the information systems shall be granted only after authenticating visitors before authorizing access to the facility where the information systems reside other than areas designated as "publicly accessible".

17. The access records of the visitors shall be maintained.

18. Visitors shall be escorted by the designated personnel and their activities, if required, shall be monitored.

19. Any user who needs to connect to the external network for official work shall be able to do so after an official sanction from the Management and Security Team. This team shall evaluate security risks before issuing any sanction.

20. A record of all physical accesses by both visitors and authorized individuals shall be maintained.

21. All policies stated above shall be monitored for any changes from time to time.

Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the company policies.

Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months. The policy review will be undertaken by IT Department.

Acknowledgment

This form is used to acknowledge receipt of, and compliance with, the Automated Services Network Co. Physical Security Policy.

Signature

By signing below, I agree to the following terms:

I have received and read a copy of the "Physical Security Policy" and understand the same.
I confirm that the above have read and received and read a copy of the "Physical Security Policy" and agree to comply to it.

Full Name	Designation	Signature
Aashick . Noordine	Accountant	
AbdolKarim Zoheiri	Assistant Business Development Manager	
Abdul Raheem Mohammad	Network Administrator	
Abdullah Ahmad Ebrahim	Credit Unit Manager	
Abdulrahman Mohamed ElRotel	Financial Manager	
Afaf samy AlShafie	Applications Developer	afaf alshafie
Afif Hussein Mukahal	Executive Manager	
Ahmed Ahmed Soliman	Sales Executive	
Ahmed Ebraheem Daloq	Logistics Officer	