شركة شبكة الخدمات الآلية
Automated Services Network Co.

Information Systems Access Policy

Version: 1.6

Approved Date: 12-8-2025

Approved by:

Sabah Khaled Al-Ghunaim

Chairman

شركة شبكة الخدمات الآلية
Automated Services Network Co.

Contents

1. Policy Statement

Automated Services Network Company (eNet) will establish specific requirements for protecting information and information systems against unauthorized access. eNet will effectively communicate the need for information and information system access control.

2. Purpose

Information security is the protection of information against accidental or malicious disclosure, modification, or destruction. Information is an important asset of eNet that must be managed with care. All information has value to the organization. However, not all this information has equal value or requires the same level of protection. Access controls are put in place to protect information by controlling who has the right to use different information resources and by guarding against unauthorized use. Formal procedures must control how access to information is granted and how such access is changed. This policy also mandates a standard for the creation of strong passwords, their protection, and frequency of change.

3. Scope

This policy applies to all eNet Organization, Committees, Departments, Partners, Employees of the Organization (including system support staff with access to privileged administrative passwords), contractual third parties and agents of the Organization with any form of access to [Organization Name's] information and information systems.

4. Definition

Access control rules and procedures are required to regulate who can access eNet information resources or systems and the associated access privileges. This policy always applies and should be adhered to whenever accessing eNet information in any format, and on any device.

5. Risks

On occasion business information may be disclosed or accessed prematurely, accidentally, or unlawfully. Individuals or companies, without the correct authorization and clearance, may intentionally or accidentally gain unauthorized access to business information which may adversely affect day-to-day business. This policy is intended to mitigate that risk. Non-compliance with this policy could have a significant effect on the efficient operation of the Organization and may result in financial loss and an inability to provide necessary services to our customers.

6. Applying the Policy – Passwords

6.1 Choosing Passwords

Passwords are the first line of defence for our ICT systems and together with the user ID helps to establish that people are who they claim to be. A poorly chosen or misused password is a security risk and may impact the confidentiality, integrity, or availability of our computers and systems.

Weak and strong passwords

A weak password is one that is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers, and simple patterns of letters from a computer keyboard. A strong password is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer. Everyone must use strong passwords with a minimum standard of password controls which includes but is not limited to:

- Minimum password length of 8 to 10 characters.
- Minimum password age of 1 day
- Maximum password age of 90 days
- Password history of 6 passwords
- Password encryption applied

6.2 Protecting Passwords

It is of utmost importance that the password always remains protected. The following guidelines must be always adhered to:

- Never reveal your passwords to anyone.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different eNet systems.
- Do not use the same password for systems inside and outside of work.

6.3 Changing Passwords

All user-level passwords must be changed at a maximum of every 90 days, or whenever a system prompts you to change it. Default passwords must also be changed immediately. If you become aware or suspect, that your password has become known to someone else, you must change it immediately and report your concern to IT Department. Users must not reuse the same password within 20 password changes.

6.4 System Administration Standards

The password administration process for individual eNet systems is well-documented and available to designated individuals. All eNet IT systems will be configured to enforce the following:

- Authentication of individual users, not groups of users – i.e., no generic accounts.
- Protection with regards to the retrieval of passwords and security details.
- System access monitoring and logging – at a user level.
- Role management so that functions can be performed without sharing passwords.
- Password admin processes must be properly controlled, secure and auditable.

7. Applying the Policy – Employee Access

7.1 User Access Management

Formal user access control procedures must be documented, implemented, and kept up to date for each application and information system to ensure authorized user access and to prevent unauthorized access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. These must be agreed upon by eNet. Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

7.2 User Registration

A request for access to the Organization's computer systems must first be submitted to the head of IT department for approval. Applications for access must only be submitted if approval has been gained from IT Manager.

When an employee leaves the organization, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of the HR Manager to request the suspension of the access rights via the IT Department.

7.3 User Responsibilities

It is a user's responsibility to prevent their user-ID and password is used to gain unauthorized access to Organization systems by:

- Following the Password Policy Statements outlined above in Section 6.
- Ensuring that any PC they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing IT Department of any changes to their role and access requirements.

7.4 Network Access Control

The use of modems on non-Organization-owned PCs connected to the Organization's network can seriously compromise the security of the network. The normal operation of the network must not be interfered with. Specific approval must be obtained from IT Manager before connecting any equipment to the Organization's network.

7.5 User Authentication for External Connections

Where remote access to the eNet network is required, an application must be made via the IT Department. Remote access to the network must be secured by two-factor authentication consisting of a username and VPN authentication token.

7.6 Supplier's Remote Access to the Organization Network

Partner agencies or 3rd party suppliers must not be given details of how to access the Organization's network without permission from IT Department. Any changes to supplier's connections must be immediately sent to the IT Manager so that access can be updated or ceased. All permissions and access methods must be controlled by IT Department.

Partners or 3rd party suppliers must contact the IT Department before connecting to the eNet network and a log of activity must be maintained. Remote access software must be disabled when not in use.

7.7 Operating System Access Control

Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section (section 7.1) and the Password section (section 6) above must be applied. The login procedure must also be protected by:

- Not displaying any previous login information e.g., username.
- Limiting the number of unsuccessful attempts and locking the account, if exceeded.

- The password characters being hidden by symbols.
- Displaying a general warning notice that only authorized users are allowed.

All-access to operating systems is via a unique login id that will be audited and can be traced back to each individual user. The login id must not give any indication of the level of access that it provides to the system (e.g., administration rights). System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day-to-day activities.

7.8 Application and Information Access

Access within software applications must be restricted using the security features built into the individual product. The IT Department of the software application is responsible for granting access to the information within the system. The access must:

- Be compliant with the User Access Management section (section 7.1) and the Password section (section 6) above.
- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.
- Be unable to be overridden (with the admin settings removed or hidden from the user).
- Be free from alteration by rights inherited from the operating system that could allow unauthorized higher levels of access.
- Be logged and auditable.

8. Policy Compliance

If any user is found to have breached this policy, they may be subject to company's disciplinary procedure. If a criminal offense is considered to have been committed further action may be taken to assist in the prosecution of the offender(s). If you do not understand the implications of this policy or how it may apply to you, seek advice from [name appropriate department].

9. Policy Governance

The following table identifies who within eNet is Accountable, Responsible, Informed, or Consulted with regards to this policy. The following definitions apply:

- Responsible – the person(s) responsible for developing and implementing the policy.
- Accountable – the person who has ultimate accountability and authority for the policy.
- Consulted – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- Informed – the person(s) or groups to be informed after policy implementation or amendment.

Responsible, Head of IT Department
Accountable, the General Manager of the company
Consulted, the Chairman of the company and BOD.
Informed, All Organization Employees and all Temporary Staff.

10. 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.

11. Key Messages

- All users must use strong passwords.
- Passwords must be always protected and must be changed at least every 90 days.
- User access rights must be reviewed at regular intervals.
- It is a user's responsibility to prevent their user-ID and password is being used to gain unauthorized access to Organization systems.
- Partner agencies or 3rd party suppliers must not be given details of how to access the Organization's network without permission from IT Department.
- Partners or 3rd party suppliers must contact the IT Department before connecting to the eNet network.

Acknowledgment of Information Systems Access Policy

This form is used to acknowledge receipt of, and compliance with, the Automated Services Network Co. Information System Access Policy.

Signature

By signing below, I agree to the following terms:

I have received and read a copy of the "Information System Access Policy" and understand the same.

I confirm that the above have read and received and read a copy of the "Information System Access Policy" and agree to comply to it.

Full Name	Designation	Signature
Aashick . Noordine	Accountant	
Anto Oommen Chacko	Accountant	
Jinto Joy Joy	Internal Audit Manager	
Jobin Johnson Vaidyan	Accountant	
Mahmoud Abdulhalim	Accountant	
Mohamed Sanan	Logistics Officer	

Siju Abraham Oommen	Accountant	
Suku Mathew	Accountant	
Ahmed Ebraheem Daloq	Logistics Officer	
Hany Hazem Diab	Logistics Officer	
Mohamed Ahmad Nasr	Logistics Officer	
Tawfek Shonoda Tawfek	Logistics Officer	
Amira Loka	Customer Support Officer	
Asmaa Metwally	Customer Support Officer	
Mohamad Sameh Sbeiti	Customer Support Officer	
Mohammed Sayed Sadek	Customer Support Officer	
Razan Ibrahim Al Dalag	Customer Support Officer	
Realiza Usero Divina	Customer Support Officer	
Sarah Sameh Sbeity	Customer Support Officer	
Sayed ElSayed Tantawy	Customer Support Officer	
Hani Saad Radwan	Administration Officer	
Michael Mansour Basily	Compliance Manager	
Afaf samy AlShafie	Applications Developer	
Ahmed Zakzouk	Web Developer	
Akhilesh Pokkanchery	Senior Network Administrator	
Amal Abdou Abd Elaal	Web Developer	
Emad Genidy	Network Administrator	
Fahim Mahamud Parkar	Mobile Developer	
Linto Lawrance Neelamkavil	Application Support Manager	
Medhat Askander	Web Developer	
Mohamed Selmi Ali	UI/UX Designer	
Omar Mahmoud Hagras	Project Manager	
Rama Krishna Uddarraju	Information Security Manager	
Reham Abdulhalim Ali	Web Developer	
Salma Rizk El-Etripy	Software Tester	
Shahad Sawas	Software Tester	
Syed . Hussain	Net Developer	
Abdulrahman ElRotel	Financial Manager	
Afif Hussein Mukahal	Executive Manager	

Jamal Eldeen A. Kubeer	General Manager	
Khaled Al Ghunaim	Board Member	
Nesrine Zakaria	Executive Manager	
Sabah Al Ghunaim	Chairman	
Ahmed Soliman	Sales Executive	
Ahmed Al Gendy	Sales Executive	
Anwar Al Furaih	Sales Executive	
Danah AlHumoud	Sales Executive	
Elsayed Thabet	Risk Manager	
Jamal Mahmoud Ibrahim	Sales Executive	
Mohammad Al Shatti	Sales Executive	
Muzammil AbdulMannan	Business Development Manager	
Nouf Bader J. Al Bahar	Sales Executive	
Shoug Sabah Al Ghunaim	Sales Executive	
Ali Khaleel Mohamed	Technical Support Engineer	