شركة شبكة الخدمات الآلية
Automated Services Network Co.

Information Security Policy

Version: 1.8

Date: 11-11-2025

Approved by:

Sabah Khaled Al-Ghunaim
Chairman

شركة شبكة الخدمات الآلية
Automated Services Network Co.

Table of Contents

Introduction

Computer information systems and networks are an integral part of business at **Automated Services Network Co. (eNet).** The company has made a substantial investment in human and financial resources to create these systems.

The enclosed policies and directives have been established in order to:

- Protect eNet investment.
- Safeguard the information contained within systems.
- Reduce business and legal risk.
- Protect the good name of the company.

Scope of Policy

This policy applies to all our employees; manager, administrators, customer support, sales and any employee or who has permanent or temporary access to our systems and hardware.

Administration

The information technology department (IT department) is responsible for the administration of this policy.

Violations

Violations may result in disciplinary action in accordance with company policy. Failure to observe these guidelines may result in disciplinary action by the company depending upon the type and severity of the violation, whether it causes any liability or loss to the company, and/or the presence of any repeated violation(s).

Statement of responsibility

General responsibilities pertaining to this policy are set forth in this section. The following sections list additional specific responsibilities.

Manager responsibilities

Managers and supervisors must:

Ensure that all appropriate personnel are aware of and comply with this policy.
Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees adhere to this policy.

IT department responsibilities

The IT department must:

1. Develop and maintain standards and procedures necessary to ensure implementation of and compliance with the policy directives.
2. Provide appropriate support and guidance to assist employees to fulfill their responsibilities under its directive.

1- The Internet and e-mail

Access to the Internet is provided to employees for the benefit of **Automated Services Network Co.** and its customers. To ensure that all employees are responsible and productive Internet users and to protect the company's interests, the following guidelines have been established for using the Internet and e-mail.

Acceptable use

Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

- Using web browsers to obtain business information from the web.
- Handling the customer support.
- Accessing eNet systems for information as needed.
- Using e-mail in business communication.

Unacceptable use

Employees must not use the Internet for purposes that are illegal, unethical, harmful to the company, or nonproductive. Examples of unacceptable use are:

- Broadcasting e-mail or sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
- Conducting a personal business using company resources.
- Transmitting any content that is offensive, harassing, or fraudulent.

Downloads

Downloads from the Internet are highly restricted and is managed by system administrators only.

Employee responsibilities

An employee who uses the Internet or Internet e-mail shall:

1. Ensure that communications are for professional reasons and they do not interfere with his/her productivity.
2. Be responsible for the content of all text, audio, or images that he/she places or sends over the Internet. All communications should include the employee's name and position.
3. Not transmit copyrighted materials without permission.
4. Know and abide by all applicable company policies dealing with security and confidentiality of eNet records.
5. Ensure running a virus scan on any executable file(s) received through the Internet.
6. Avoid transmission of nonpublic customer information. If it is necessary to transmit nonpublic information, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use.

Copyrights

Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the company and/or legal action by the copyright owner.

Monitoring

All messages created, sent, or retrieved over the Internet are the property of the company and *may be regarded as public information*. **Automated Services Network Co.** reserves the right to access the contents of any messages sent over its facilities if the company believes, in its sole judgment, that it has a business need to do so. All communications, including text and images, can be disclosed to law enforcement without prior consent of the sender or the receiver.

Audit and Review

The information security team may conduct review on regular basis to ensure the policy is enforced.

2- Computer viruses

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of corporate resources.

Background

It is important to know that:

- Computer viruses are much easier to prevent than to cure.

- Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

IT responsibilities

IT shall:

1. Install and maintain appropriate antivirus software on all computers.
2. Respond to all virus attacks, destroy any virus detected, and document each incident.

Employee responsibilities

These directives apply to all employees:

1. Employees shall not knowingly introduce a computer virus into company computers.
2. Employees shall not load any external storage devices (hard drives, CD's, flash drives, etc) of unknown origin.
3. Incoming external storage devices shall be scanned for viruses before they are read.
4. Any associate who suspects that his/her computer has been infected by a virus shall IMMEDIATELY POWER OFF the computer and call the IT administrator.

3- Spyware

Spyware and adware can compromise system performance, as a result, combating spyware requires user vigilance as well as IT management and control.

IT responsibilities

1. Install and configure auto update appropriate anti-spyware software on all computers.
2. Respond to all reports of spyware installation, remove spyware modules, restore system functionality, and document each incident.

Employee responsibilities

These directives apply to all employees:

1. Employees shall not knowingly allow spyware to install on company computers.
2. Employees shall immediately report any symptoms that suggest spyware may have been installed on their computer.

4- Access codes and passwords

The confidentiality and integrity of data stored on company computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties.

IT responsibilities

The IT manager shall be responsible for the administration of access controls to all company computer systems. The IT manager will process adds, deletions, and changes upon receipt of a written request from the end user's supervisor. The IT manager will implement a complex password policy into domain servers.

Deletions of user's access may be processed by an oral request prior to reception of the written request. The IT manager will maintain a list of administrative access codes and passwords and keep this list in a secure area.

Employee responsibilities

Each employee:

1. Shall be responsible for all computer transactions that are made with his/her User ID and password.
2. Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded where they may be easily obtained.
3. Will change passwords at least every 90 days.
4. Should use passwords that will not be easily guessed by others.
5. Should log out or lock the computer when leaving a computer for an extended period.
6. Should not attempt to access the accounts of other users

Supervisor's responsibility

Managers and supervisors should notify the IT manager promptly whenever an employee leaves the company or transfers to another department so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

Human resources responsibility

The human resources department will notify the IT department monthly of associate transfers and terminations. Involuntary terminations must be reported concurrent with the termination.

5- Physical security

It is company policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

Employee responsibilities

The directives below apply to all employees:

1. CD's and portable storage devices should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.
2. CD's and portable storage devices should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
3. Critical computer equipment, e.g., file servers, must be protected by an uninterruptible power supply (UPS).
4. Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
5. Since the IT administrators are responsible for all equipment installations, disconnections, modifications, and relocations, employees are not to perform these activities.
6. Employees shall not take shared portable equipment such as laptop computers out of the company premises without the informed consent of their department manager. Informed consent means that the manager knows what equipment is leaving, what data is on it, and for what purpose it will be used.
7. Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result.

6- Copyrights and license agreements

eNet complies to all laws regarding intellectual property. Employees are legally bound to comply with the Government Copyright Act and all proprietary software license agreements. Noncompliance can expose the company and the responsible employee(s) to civil and/or criminal penalties.

Scope

This directive applies to all software that is owned by eNet or licensed to Automated Services Network Co. or developed using eNet resources by employees or vendors.

IT responsibilities

The IT manager will:

1. Maintain records of software licenses owned by eNet.
2. Periodically (at least annually) scan company computers to verify that only authorized software is installed.

Employee responsibilities

Employees shall not:

1. Install software unless authorized by IT. Only software that is licensed to or owned by eNet is to be installed on eNet computers.
2. Copy software unless authorized by IT.
3. Download software unless authorized by IT.

Civil penalties

Violations of copyright law expose the company and the responsible employee(s) to the following penalties:

- Liability for damages suffered by the copyright owner
- Profits that are attributable to the copying
- Fines for each illegal copy.

Criminal penalties

Violations of copyright law that are committed "willfully and for purposes of commercial advantage or private financial gain," expose the company and the employee(s) responsible to the following criminal penalties:

- Fines for each illegal copy
- Jail terms.

7- Remote Access

Participation in a remote access program may not be possible for every employee. Remote access is meant to be an alternative method of meeting company needs. The company may refuse to extend remote access privileges to any employee or terminate a remote access arrangement at any time.

Acceptable Use

Hardware devices, software programs, and network systems purchased and provided by the company for remote access are to be used only for creating, researching, and processing company-related materials. By using the company's hardware, software, and network systems the user assumes personal responsibility for their appropriate use and agree to comply with the policy and other applicable company policies, as well as governmental laws and regulations.

Your eligibility to remotely access the company's computer network will be determined by your manager.

Equipment & Tools

The company may provide tools and equipments for remotely accessing the corporate computer network. This may include computer hardware, software, phone lines, e-mail, voicemail, connectivity to host applications, and other applicable equipment as deemed necessary.

The use of equipment and software provided by the company for remotely accessing the company's computer network is limited to authorized persons and for purposes relating to company business. The company will provide repairs to company equipment. When the employee uses her/his own equipment, the employee is responsible for maintenance and repair of his/her equipment.

Use of personal computers and equipment

Remote access to the company network by any employee on a personal computer that does not belong to company is prohibited. The company employee is responsible to ensure not to perform any illegal activities and not to use the access for outside business interests. The employee bears responsibility for the consequences should the access be misused.

Violations and Penalties

Violating the Remote Access Policy could result in disciplinary action leading up to include termination of employment and civil and/or criminal prosecution under Governmental laws.

8- Software Installation Policy

Installation of unauthorized computer programs and software, including files downloaded and accessed, can easily and quickly introduce serious, fast-spreading security vulnerabilities. Unauthorized software programs, even those seemingly provided by reputable vendors and trusted companies, can introduce viruses and Trojan programs that aid hackers' attempts to illegally obtain sensitive, proprietary, and confidential data. Protecting eNet's computers, systems, data, and communications from unauthorized access and guarding against data loss is of paramount importance; adherence to the following Software Installation Policy serves a critical role in the process.

Purpose

This policy's purpose is to ensure every employee, contractor, temporary worker, etc. understands, and agrees to abide by, specific guidelines for software, program and application installation and use on eNet-provided computers, systems, and networks.

Scope

eNet's Software Installation Policy applies to all employees, contractors, temporary workers, and others that operate eNet-owned computers, access eNet-provided Internet services or access eNet-provided electronic or instant messaging services. All use of eNet's user accounts, desktop computers, notebook PCs, servers, Internet, and messaging services must conform to the guidelines presented in this policy.

Approved Software Applications

eNet's information technology department tests and approves the use of only specific software programs and applications, including updates and patches to existing installed applications. Only the information technology department will install approved software programs, applications, and updates on all eNet systems and for those users requiring those programs and applications. The installation and use of any unauthorized applications is prohibited. Employees and other users must obtain written departmental approval prior to requesting any unauthorized software or using any unapproved application on any eNet-provided equipment or systems, except for the named following software applications:

- Adobe Acrobat Reader.
- Microsoft Internet Explorer Browser.
- Microsoft Office (Word, Excel, PowerPoint, Outlook.)
- ESET Antivirus.

Acceptable Use

eNet provides software programs and applications as a means of increasing productivity, enabling electronic communications, and transacting business. Software programs and applications are provided as required to employees, contractors, temporary workers, and other authorized agents only for the performance and fulfillment of job responsibilities. Software programs and applications are neither provided nor supported for non-business activities; eNet's software programs and applications are not to be used for personal activities.

Prohibited Software

eNet's computer systems, networks and information technology services are provided as a means of fulfilling job tasks and responsibilities. eNet places a priority on ensuring all installed software and applications are properly tested and licensed. Users are prohibited from installing any software programs and applications (other than those expressly listed in the Approved Software Applications section), including software purchased for personal use.

Under no circumstances are users to download, install, copy, access, execute or otherwise employ any of the following:

- Illegal software or programs.
- Unlicensed applications.
- Unapproved or unlicensed operating systems.
- Pirated software.
- Software purchased for personal or home use.

Ownership

eNet provides software applications and programs as productivity enhancement tools. All eNet-provided software and licenses remain eNet's property. If requested, users must surrender in a timely manner software license, software disks, CD-ROMs and DVDs and other software and application materials provided by eNet and discontinue their use. Under no circumstances are users to make illegal copies of software, applications, or programs.

Violations and Penalties

Violations of the Software Installation Policy could result in disciplinary action leading up to and including termination of employment and civil and/or criminal prosecution under Governmental laws.

9- Instant Messaging Policy

Instant messaging (IM) systems introduce a serious security risk often exploited by hackers. IM programs can introduce viruses and trojan programs that aid hackers' attempts to illegally obtain sensitive and confidential data. Protecting eNet's computers, systems, data, and communications from unauthorized access is of paramount importance; adherence to the following IM guidelines plays a critical role in the process.

Scope

eNet's Instant Messaging Policy applies to all employees, contractors, temporary workers, and others that operate eNet-owned computers, access eNet-provided Internet services or access eNet-provided electronic or instant messaging services. All use of eNet's user accounts, desktop computers, notebook PCs, servers, Internet, and messaging services must conform to the guidelines presented in this policy.

IM Applications and Installation

eNet's information technology department approves the use of only specific instant messaging applications. The information technology department will install approved instant messaging applications on all eNet systems requiring instant messaging software. The installation and use of any unauthorized Instant Messaging application is prohibited. Employees and other users must obtain departmental approval prior to requesting any IM software or using an IM application on any eNet-provided equipment or systems.

Acceptable Use

eNet provides instant messaging applications and services as a means of increasing productivity, enabling electronic communications and transacting business. Instant messaging applications and services are provided as required to employees, contractors, temporary workers, and other authorized agents only for the performance and fulfillment of job responsibilities. Instant messaging services are neither provided nor supported for non-business activities; eNet's instant messaging systems are not to be used for personal activities.

Monitoring

Instant messaging offers an opportunity for non-authorized users to view or access eNet information, including proprietary, sensitive, and confidential data. To properly audit and secure its network, systems, computers, and data, eNet monitors instant messaging use; eNet may, at its discretion and without notice, monitor employee, contractor, temporary worker, and other use of instant messaging services at any time. Information and instant message communications passing through or stored on eNet equipment can and will be monitored and will be archived for storage. Users should have no expectation of privacy when using eNet-owned, eNet-leased, or eNet-provided instant messaging services.

Ownership

As a productivity enhancement tool, all instant messages, including backup and archive copies, sent, or received using eNet-provided systems become the property of eNet. Instant messages sent or received using eNet-provided accounts or systems are not the property of users. If requested, employees and others must surrender all IM-related material to eNet in a timely manner and discontinue use of eNet-based account.

Violations and Penalties

Violations of the Instant Messaging Policy could result in disciplinary action leading up to and including termination of employment and civil and/or criminal prosecution under governmental laws.

10- IT Security Assessment

Purpose

To empower eNet to perform periodic IT security assessments ISA for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

Scope

Security assessments can be conducted on any entity within the company or any outside entity that has signed a *Third-Party Agreement* with the company. ISA can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained. It also should include following types of assessment:

- Vulnerability Assessment
- Security Audits
- Penetration Testing
- Risk Assessment

Policy

The execution, development and implementation of remediation programs is the joint responsibility of eNet and the department responsible for the systems are being assessed. Employees are expected to cooperate fully with any ISA being conducted on systems for which they are held accountable. Employees are further expected to work with eNet Assessment Team in the development of a remediation plan.

The assessment should be performed periodically each quarter or when needed.

Violations and Penalties

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

11- 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 of Information Security Policy

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

Procedure

Complete the following steps:

1. Read the Information Security Policy.
2. Sign and date in the spaces provided below.
3. Return this page only to the information services manager.

Signature

By signing below, I agree to the following terms:

i. I have received and read a copy of the "Information Security Policy" and understand the same;

ii. I understand and agree that any computers, software, and storage media provided to me by the company contains proprietary and confidential information about **Automated Services Network Co.** and its customers or its vendors, and that this is always and remains the property of the company.

iii. I agree that I shall not copy, duplicate (except for backup purposes as part of my job here at **Automated Services Network Co.**), otherwise disclose, or allow anyone else to copy or duplicate any of this information or software.

iv. I agree that, if I leave **Automated Services Network Co.** for any reason, I shall immediately return to the company the original and copies of all software, computer materials, or computer equipment that I may have received from the company that is either in my possession or otherwise directly or indirectly under my control.

I confirm that the above have read and received and read a copy of the "Information Security 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 Vaidyan	Accountant	
Mahmoud Abdulhalim	Accountant	
Mohamed Hassan A. Sanan	Logistics Officer	
Siju Abraham Oommen	Accountant	
Suku Mathew	Accountant	
Amira Loka	Customer Support Officer	
Asmaa Metwally	Customer Support Officer	Asmaa

Mohamad Sameh Sbeiti	Customer Support Officer	
Mohammed Sayed Sadek	Customer Support Officer	
Razan Ibrahim Al Dalag	Customer Support Officer	
Sarah Sameh Sbeity	Customer Support Officer	
Hani Saad Radwan	Administration Officer	
Michael Mansour Basily	Compliance Manager	
Akhilesh Pokkanchery	Senior Network Administrator	
Emad Genidy	Network Administrator	
Fahim Mahamud Parkar	Mobile Developer	
Linto Lawrance Neelamkavil	Application Support Manager	
Medhat Merzk Zaki Askander	Web Developer	
Omar Mahmoud Hagras	Project Manager	
Rama Krishna Uddarraju	Information Security Manager	
Shahad Abdulwahab Sawas	Software Tester	
Syed . Hussain	Net Developer	
Abdulrahman Mohamed ElRotel	Financial Manager	
Afif Hussein Mukahal	Executive Manager	
Jamal Eldeen A. Kubeer	General Manager	
Khaled Al Ghunaim	Executive Manager	
Nesrine Zakaria Emam	Executive Manager	
Sabah Al Ghunaim	Chairman	
Ahmed Ahmed Soliman	Sales Executive	
Ahmed Hassan Al-Gendy	Sales Executive	
Anwar A. Aziz Al Furaih	Sales Executive	
Danah Abdulrahman AlHumoud	Sales Executive	
Elsayed Mohammed Thabet	Risk Manager	
Jamal Mahmoud Ibrahim	Sales Executive	
Mohammad Mousa Awadh Al Shatti	Sales Executive	
Muzammil ahmed AbdulMannan	Business Development Manager	
Nouf Bader J. Al Bahar	Sales Executive	
Sayed ElSayed Tantawy	Sales Executive	
Shoug Sabah Al Ghunaim	Sales Executive	
Yousef Mohammad Al Temeemi	Sales Executive	
Ali Khaleel Mohamed	Technical Support Engineer	
Walid Hamed ElAzab	Technical Support	

Reham Abdulhalim Ali	Web Developer	Reham Ahmed
Salma Rizk El-Etripy	Software Tester	
Amal Abdou Abd Elaal	Web Developer	Amal Ahmed
Afaf samy AlShafie	Applications Developer	afaf alshafie
Ahmed Zakzouk	Web Developer	
Mohamed Selmi Ali	UI/UX Designer	