



**ENERGY SACCO SAVINGS AND CREDIT CO-OPERATIVE SOCIETY LTD.**

## **CYBER SECURITY POLICY**

**23 May 2022**

A handwritten signature in black ink, appearing to be 'K. K. K.', written in a cursive style.

A handwritten signature in black ink, appearing to be 'A. A. A.', written in a cursive style.

A handwritten signature in blue ink, consisting of a long horizontal stroke followed by several vertical lines.

## Table of Contents

1. Citation.....	3
2. Introduction .....	3
2.1 Context:.....	3
2.2 Definition of Key terminologies .....	4
3. Scope and Purpose of Cyber Security Policy.....	5
3.1 Scope.....	5
3.2 Purpose of the Policy .....	6
3.3 Goals of the Policy.....	6
3.4 Objective of the Policy .....	6
4. Approaches to Securing Mobile Banking Service Provision.....	6
5. Cybersecurity measures to be implemented.....	7
5.1 Confidential Data .....	7
5.2 Protect Personal and Sacco Devices .....	7
5.3 Safekeeping Emails.....	8
5.4 Managing Passwords.....	8
5.5 Data Transfers .....	8
5.6 Security Audits .....	8
5.7 Insider Threats Management.....	9
6. Authorization and access control policy .....	9
6.1 Policy Refinement .....	9
6.2 Access to Sacco servers.....	10
6.3 Security Awareness and Behavior.....	10
6.4 Responsibilities, Rights, and Duties of the Board .....	10
6.5 Responsibilities of the Management .....	10
7. Delegation of Authority.....	10
8. Approval of the Policy .....	11

1. Citation

This policy shall be called the '**Cyber Security policy**' of Energy Cooperative Savings and Credit Society Ltd. herein after referred to as '**the Society**'.

2. Introduction

This cyber security policy includes guidelines and provisions for security measures to help security risk. It applies to Sacco employees, contractors, interns/attachees and anyone who has permanent or temporary access to the Sacco systems and hardware.

A cybersecurity framework is a system of standards, guidelines and best practices for managing digital risk. Frameworks typically match specific security objectives with rules and guidelines related to the security of the information stored digitally at any point in the network or within the Sacco's boundaries of authority. In this policy, cyber security is interchangeably used with information security.

It is recognized that Savings and Credit Cooperatives (SACCOs) are utilizing the opportunities offered by advances in ICTs to ensure their operations are user friendly, their products and services are competitive, and develop customer-centric strategies. The ubiquitous and universal access to information and services together with a possibility for a unique and personalized exchange of information provided by mobile services have an impact on consumers.

While connectivity is indispensable for achieving such business success, SACCOs get exposed to a myriad of cyber-security challenges to mobile banking which when exploited lead to violation of Confidentiality, Integrity and Availability that erodes down the user perceived secure mobile banking service delivery. Cybercrime has increasingly led Saccos and financial institutions into unexplained loss of money.

2.1 Context:

With the evolution of the Internet and networks in organization, there is an immediate need for current security measures and polices to reduce the threats and challenges emerging from new technologies namely software application and network devices. The lack of cyber security awareness among technology users puts Kenyan organizations and Energy Sacco in particular, in a critical challenge. Employees, Board Members, other leaders and customers have limited knowledge of the level of risk they are exposing themselves and their Sacco to.

The problem Information security efforts will continue to be challenged by the rapid technological change and the increasing sophisticated nature of threats. While the Sacco may be aware of basics, the threat landscape is constantly evolving, creating a challenge to keep up with current developments amid competitive pressure to integrate new technologies into the Sacco's financial operations. In light of the challenges posed, Energy Sacco commits to responding to the fast changes in the financial environment and adopting new Information Technology (IT) approaches to the SACCOS' information security. In the recent past, cyber related fraud has been observed and currently under forensic investigation. This has brought into the fore the need for a cyber security policy to forestall future incidents perpetrated through the information security systems.

The Board of Energy Cooperative Savings and Credit Society Ltd, recognizing that it is solely responsible for supervision of the Society's inevitable application of information technology adopts this policy for governing the use of ICT in its operations.

## 2.2 Definition of Key terminologies

**Authentication:** The process of determining the identity of an individual or device

**Availability:** Ensuring accessibility of information to authorized users when required or information that is accessible when required by the business process now and in the future.

**Accountability:** an essential part of an information security plan. The phrase means that every individual who works with an information system should have specific responsibilities for information assurance.

**Business process reengineering (BPR):** A management technique used to improve the efficiency and effectiveness of a process within an organization

**Confidentiality:** Limiting access to information/data to authorized users only or the protection of sensitive or private information from unauthorized disclosure.

**Continuous Improvement:** An ad hoc, ongoing effort to improve business products, services, or processes

**cybersecurity framework:** a system of standards, guidelines and best practices for managing digital risk. Frameworks typically match specific security objectives with

**Cyber Security:** the collection of policies, security safeguards, risk management approaches, guidelines, technologies, actions and training that can be used to protect the organization and cyber environment together with the user's assets.

**Cyber-crime:** the use of computers and related devices and the Internet to commit a crime, usually targeting individuals or groups with the motivation to cause physical or mental harm, diminish the reputation of the victim, cause loss of money, or even gain access to sensitive information.

**Governance:** The act of managing implementation and compliance with organization policies

**Information Assurance:** The implementation of controls designed to ensure confidentiality, integrity, availability, and non-repudiation

**Information Systems Security:** The act of protecting information systems or IT infrastructures from unauthorized use, access, disruption, or destruction

**Information Systems Security Management Life Cycle:** The five-phase management process of controlling the Planning, Implementation, Evaluation and Maintenance of information systems security.

**Information Security Policies:** Information security policies pertain to written documentation outlining the structure of the organization's security posture. The purpose of information security entails the preservation of confidentiality, integrity and availability. Elements of information security include authenticity, accountability, non-repudiation and reliability. Subsequently, security policies provide guidance with regard to the physical and remote access to data of the SACCOS.

**Integrity:** The act of ensuring that information has not been improperly changed. It also refers to the accuracy, completeness and validity of information.

**Insider Threats:** an insider threat is a current or former employee, contractor, Board member, or business partner who has or had authorized access to an organization's network, system, or data or who leak or share information with unauthorized parties. Insider refers to someone working or directly interacting with Sacco operations who may pose a risk to you if they make a mistake with data handling procedures.

**Need to know:** A principle that restricts information access to only users with an approved and valid requirement

**Non-repudiation:** The concept of applying technology in a way that an individual cannot deny or dispute they were part of a transaction.

**Phishing:** impersonating a trusted third party by a phisher in order to gain access to private information.

**Policy:** A document that states how the organization is to perform and conduct business functions and transactions with a desired outcome

**Policy Framework:** A structure for organizing policies , standards , procedures, and guidelines

**Procedure:** A written statement describing the steps required to implement a process

**Security Policies:** A set of policies that establish how an organization secures its facilities and IT infrastructure. Can also address how the organization meets regulatory requirements

**Service Level Agreement (SLA):** The portion of a service contract that formally defines the level of service. These agreements are typical in telecommunications contracts for voice and data transmission circuits

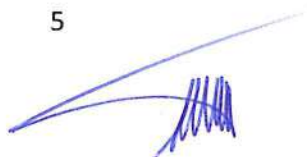
**Standard:** An established and proven norm or method. This can be a procedural standard pr a technical standard implemented organization-wide.

### 3. Scope and Purpose of Cyber Security Policy

The Board shall ensure that this policy statement complies at all times with the provisions of the Cooperative Societies Act, the Rules, Society by-laws and any other laws or regulations enacted and or recognized in Kenya.

#### 3.1 Scope

The scope of this policy includes: address all data, programs, systems, facilities, authenticity, accountability, non-repudiation, reliability of information security and other technology infrastructure, users of technology and third parties in the Sacco without exception. It also includes information protection, information systems security, Internet use, network security, privacy, physical security, remote access, system administration security and incident response procedures and the method of reporting incidents relative to insider security breaches and attendant consequences as well as provision of guidance with regard to the physical and remote access to data of the SACCO.



### 3.2 Purpose of the Policy

The purpose of this policy is to:

- Detect and forestall the compromise of information security such as misuse of data, networks, computer systems and applications.
- Creating an overall approach to ensure information security
- Observe the rights of the customers, which include how to react to inquiries and complaints about non-compliance
- Maintaining the reputation of the Sacco, and uphold its ethical and legal responsibilities.
- To establish a general approach to information security
- Providing effective mechanisms for responding to complaints and queries concerning real or perceived non-compliances with the policy is one way to achieve this objective

### 3.3 Goals of the Policy

That authorized users can access the information communication technology network and information resources to support of Energy Sacco operations. Additionally, the Sacco Employees, Board and General membership the benefits and penalties of appropriate and inappropriate behavior when using SACCOS' information resources and/or assets, respectively.

### 3.4 Objective of the Policy

The principal objective of information security is to safeguard the availability, integrity, and confidentiality of information.

## 4. Approaches to Securing Mobile Banking Service Provision

In order to effectively defend against cyber-attacks, a multifaceted approach will be used. It will be achieved through physical security mechanisms, technical controls, security policy and education and training.


### **Access Control**

Access control will be put in place to allow only authenticated users to gain access and keep the rest off. This will be achieved through use of double passwords control. The double password control includes the log-in password and the transaction for the log-in password a mixture of numbers and letters needs to be used and this means confidentiality is ensured to a certain degree and this is limited to log in. The transaction password on the other hand is required when users need to transfer funds.

### **Technical Controls**

One of the technical controls to be employed is the use of firewalls. Firewalls employ a combination of computer hardware and software that is designed to separate the Internet from the Internal Web servers, networks, computer systems and databases securely. Back-up and recovery will be another technical control. An off-site back up will be established for recovery from major failures to ensure continuity in business operations.

### **Education and Training**



Recognizing that People's vulnerability to cyber security is contributed by their lack of awareness to the types of social engineering attacks, all employees, board members and other leaders who directly interact with the Sacco information technology will be educated and trained constantly to improve their knowledge of threats that are often cited as critical to enhance cyber security.

#### 5. Cybersecurity measures to be implemented

- i. Training and educating the staff and customers about cybercrime threats
- ii. Separating, encrypting, and backing up data
- iii. Regularly upgrading the Information Communication Technology (ICT)
- iv. Performing regular security audit of the system to determine vulnerabilities, hence make amends before cybercrime happens
- v. Strengthen ICT control systems and review contracts signed with software vendors to compel such dealers to be compensating the co-operatives when losses occur.
- vi. Conducting due diligence on vendors before engaging them

#### 5.1 Confidential Data

Confidential data is valuable and is to be kept secret. Sacco confidential data includes:

- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulae or new technologies
- Customer lists (existing and prospective)

#### 5.2 Protect Personal and Sacco Devices

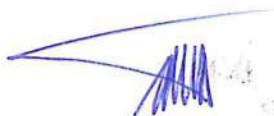
When employees use their digital devices to access company emails or accounts, they introduce new risk to company data. Employees are to keep both personal and Sacco -issued computers and cell phones secure. To keep these devices secure:

- Keep all devices password protected
- Choose and upgrade a complete antivirus software
- Do not leave devices unattended or exposed
- Log into Sacco accounts and systems through secure and private networks only

Employees are advised to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others. When newly hired staff receive Sacco-issued equipment, they will receive instructions for:

- Disk encryption setup
- Password management tool setup
- Installation of antivirus/anti malware software

Employees are to follow instructions to protect their devices and refer to Sacco security specialist or network engineer with any questions.



### 5.3 Safekeeping Emails

Emails can host scams and malicious software. To avoid virus infection or data theft employees must:

- Avoid opening attachments and clicking on links when the content is not adequately explained
- Be suspicious of click bate titles (offering prizes, advice)
- Check emails and names of people they receive messages from to ensure they are legitimate
- Look for inconsistencies, or giveaways

If an employee is not sure that an email they received is safe, they can refer to the Sacco security specialist.

### 5.4 Managing Passwords

Password leaks are dangerous, since they can compromise the sacco's entire infrastructure. Not only should passwords be secure so they are not easily hacked, but they should also remain secret. For this reason, employees are to:

- Choose passwords with at least 8 characters
- Remember passwords instead of writing them down. If they need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when the work is done
- Exchange credentials only when necessary. When exchanging them in person is not possible, employees should prefer the phone instead of email and only if they personally recognize the person they are talking to.
- Change their passwords every two months.

The Sacco will purchase the services of a password management tool which generates and stores passwords. Employees are obliged to create a secure password for the tool itself following the above-mentioned device.

### 5.5 Data Transfers

Transferring data introduces security risk. Employees must

- Avoid transferring sensitive data e.g. Customer information, employee records to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request the employees to ask the sacco's security specialist to help.
- Share confidential data over the Sacco network/system and not over public Wi-Fi or private connection
- Ensure that the recipient of the data are properly authorized people or organization and have adequate security policies
- Report scams, privacy breaches and hacking attempts

### 5.6 Security Audits

It's important to perform security audits on a regular basis to ensure that security systems, policies and procedures are effective and that no gaps exist. An effective audit will provide a comprehensive assessment of the Sacco's security and informs an ongoing process of improvement. Security audits will typically include:



- Checks to verify security procedures are being followed and security systems are not being bypassed.
- A review of past breaches to verify that a successful future attack is likely to have less impact.
- An assessment of protection against new types of threats.
- Periodic review of access rights to support enforcement of the Principal of Least Privilege.

## 5.7 Insider Threats Management

Insider threats consisting of the disgruntled or curious employees, Sacco leaders and general membership will be timely addressed when detected. The Board recognizes that insider threats are one of the most common causes of security breaches and that efforts must be made to detect these early enough.

Attendance at security policy awareness and training sessions on information security incident reporting should be required of all SACCOS' employees on an annual basis.

training attendance will be a mandatory requirement incorporated into employee evaluations in order to assure enforcement of the security policy.

Communication of the seriousness of information security responsibilities by SACCOS' management to SACCOS' employees will be critical in building a culture wherein it is second nature for employees to apply security measures.

Service providers are deemed to be potential contributors of cyber-attacks in their role of being part of the Sacco supply chain or are business partners

The Sacco considers the information management system and e-business technology systems and the networks, used for generating, storing and retrieving information as its important business assets of every organization. The security, integration and availability of information to forestall any cyber risk will be ensured.

## 6. Authorization and access control policy

Typically, the security policy will follow a hierarchical pattern. Junior staff will be required not to share the little amount of information they have unless explicitly authorized. Conversely, a senior manager may have enough authority to make a decision about what data can be shared and with whom, which means that they are not tied down by the same information security policy terms.

### 6.1 Policy Refinement

Policy refinement takes place at the same time as defining the administrative control or authority people in the organization have. Essentially, it is a hierarchy-based delegation of control in which one may have authority over his own work, a project manager has authority over project files belonging to a group he is appointed to and the system administrator has authority solely over system files.

As the IT security program matures, the policy may need updating. While doing so will not necessarily guarantee an improvement in security, it is nevertheless a sensible recommendation.

## 6.2 Access to Sacco servers

Access to the Sacco's network and servers should be via unique logins that require authentication in the form of either passwords, biometrics, ID cards or tokens etc. Monitoring on all systems must be implemented to record login attempts (both successful ones and failures) and the exact date and time of logon and logoff.

## 6.3 Security Awareness and Behavior

The Board will periodically conduct training sessions to inform employees of the Sacco cyber security methods and tools. That includes the following:

- data protection measures
- sensitive data classification
- access protection measures

## 6.4 Responsibilities, Rights, and Duties of the Board

With regard to the management of the implementation of the cyber security policy by the Sacco employees, the Board will be responsible for the following:

- access reviews
- change management
- education
- implementation
- incident management
- periodic updates of the security policy

## 6.5 Responsibilities of the Management

The society's Management will be responsible to the Board in:

- Projecting the Society's financial needs and communicating such needs to the Board
- Implementation of cybersecurity management decisions reached by the Board
- Co-ordination of Society's cyber security meetings including those by the Board
- Recommend to the Board any desired actions to enhance cyber security management actions in response to emerging technology changes
- Provision of advice to the board for the purposes of establishing and reviewing the cyber security policy.
- Recommendation to the board on the purchase or upgrade of cyber security protection software and hardware within the guidelines established in this policy.
- Communicating significant changes in factors, which may affect the attainment of the Society's cyber security objectives.

## 7. Delegation of Authority

Authority to manage the cyber security policy is granted to the CEO, through the security specialist hereinafter referred to as ICT Officer

8. Approval of the Policy

We, the undersigned, individually and collectively, give commitment to the implementation of the Investment Policy by appending our signatures on behalf of the Board of Directors.

**Signed.**

Chairman:

Name ..... Paul N. Mbuthi ..... Sign .....  ..... Date ..... 18/06/2022 .....

Secretary:

Name ..... Adia Ndumi ..... Sign .....  ..... Date ..... 18/06/2022 .....

Treasurer:

Name ..... Tom O. Oloo ..... Sign .....  ..... Date ..... 18/06/2022 .....

