Nyikwa Ezra Welfare Association
Social Welfare, Wealth, & Prosperity

NEWA Cyber Security Policy

Nyikwa Ezra Welfare Association **[N.E.W.A]**

Table of Contents

NEWA Web Application has several servers, workstations, laptops, mobile devices, point of sale terminals, and tablets. Each member has a unique login, email, and access card that includes all of their access to the systems and facilities they are allowed to access. The access granted to members is limited to the information in their personal accounts and other general information which are classified as public. Within the IT systems, there are proprietary applications tailored to the individual's role. These applications are loaded on the N.E.W.A. systems and in some cases on personal devices for those that bring their own device for work.

Each Executive has designated roles for each Member in that department, and the IT assets are designed to function according to the profile of the individual logged into that device. The Treasurer will have physical access to all financial transactions within the Web Application, but will only have access to certain IT resources as they pertain to physical security. The Chairman will have access to all data and information in the system. The Secretary General will have all access to list of members and other records but restricted access to the financial transactions. The Web Admin will have total access to all aspects of the Web Applications

General Policies and Motivation

The aim of this cyber security policy is to define policy and establish procedures related to NEWA Web Application and to provide guidance and standards for configuring and integrating the Web Application with other platforms to achieve C2B communication. The standards provided are subject to change based on new or existing requirements. The Executive must approve any changes or deviations from this policy.

This cyber security policy contains guidance and standards under the following areas:

1. Access Control
2. Physical Security
3. Email Policies
4. Breach Reporting Responsibilities
5. Mobil Policy and BYOD (Bring Your Own Device)

Section 1: Access Control Standards

Permanent or temporary access to the N.E.W.A. Web Application will be open to public. Members will be required to use their unique login, password, biometric data, or token to access their personal information, transactions, and other sensitive documents reserved for members. Executives required to use their unique login, password, biometric data, or token to access classified N.E.W.A information and documents depending on the privilege and access type extended to every executive. Below will outline the requirements for each:

Unique login Practices:

- Unique logins will include the individual's first initial, middle initial, and last name (i.e. EOOnyango).
- If an individual login duplicates another existing login, a number will be added to the end of the last name (i.e., EOOnyango1)
- Unique logins will be deactivated after 30 days of no activity or when no longer needed.
- Unique logins will be deleted after 45 days of inactivity.
- Data from unique logins will be maintained for a period of 3 years or in accordance with state and federal laws.

Password Practices:

- All passwords must be at least 14 characters long.
- Passwords must contain at least 1 upper case letter (A-Z), 1 lower case letter (a-z), 1 number (0-9), and 1 non-alphanumeric character (i.e. $,#,%)
- Passwords will expire every 60 days.
- All systems will be set remember at least 10 historical passwords that cannot be reused.
- User passwords must not be shared with anyone for any reason.
- Passwords must be different on each system the user has access to.

Biometrics Standards and Practices:

- N.E.W.A. policy is to protect and store biometric data in accordance will all state and federal laws and standards. This includes, but is not limited to, state of residence Biometric Information Privacy Acts.
- An individual's biometric data will not be collected or obtained by the corporation without prior written consent of the individual. The corporation will inform the individual for the reason the biometric data information is being collected and the length of time the data will be maintained.
- The corporation will not sell, lease, trade, or otherwise profit from an individual's biometric data.
- Biometric data will not be disclosed by the corporation without written consent from the individual, court-ordered, or disclosure is required by law.
- Biometric data will be stored using a reasonable standard of care and in a manner that meets or exceeds the N.E.W.A. standards of storing Personal Identifiable Information (PII).

- The biometric data will be destroyed when the purpose of obtaining or collecting the data has been fulfilled, or the Member is no longer with the company.

Token Standards:

- Hardware tokens will be used when necessary for IT systems as designated by the N.E.W.A. IT department guidelines.
- Hardware tokens do contain PII such as individuals name, username, email, and contact information.
- Hardware tokens must be safeguarded by individuals in such a manner that the PII will not be disclosed or lost.
- Hardware tokens will be turned in to the N.E.W.A. IT department or physical security department when no longer needed, or the individual is no longer with the company.

Section 2: Physical Security Standards

- Physical security will be maintained by all N.E.W.A. Members, temporary Members, and contracted Members.
- Physical security comprises of, but is not limited to, locked doors, access card, surveillance, alarms, and Member awareness. Below will outline the requirements for each:

Locked Door Practices:

- All doors to access the N.E.W.A. premises and within a controlled area in the premises will remain locked at all times. These doors will be accessible by individual access cards are given to all individuals as needed.
- N.E.W.A. visitors must be signed in at the access control desk and escorted by a cleared individual to the areas requested.

- Access cards must be used on all locked doors by each individual as they access that door and no “piggy backing” (using another individual’s access card) will be tolerated.

Access Card Standards and Practices:

- Access cards will be used to gain entrance to all N.E.W.A. premises and doors to certain controlled areas within the premises (i.e., IT server room).
- Access cards do contain PII such as individuals name, photograph, and contact information.
- Access cards must be safeguarded by individuals in such a manner that the PII will not be disclosed or lost.
- Access cards will be turned in to the N.E.W.A. physical security department when no longer needed, or the individual is no longer with the company.
- Lost access cards must be reported to N.E.W.A. physical security immediately so the card can be deactivated and a new one issued to the individual.

Surveillance Practices

- Surveillance of all N.E.W.A. premises will be monitored 24 hours a day and 365 days a year.
- Surveillance consists of physical security personnel roving the areas and video monitoring systems that record all activity within the premises and in the exterior of the premises.
- Video surveillance will not be conducted in areas where personal privacy is required (i.e., restrooms). But, physical security will regularly do spot checks in those areas for physical and personnel safety reasons.

- Video surveillance will be recorded and maintained on and off-site for a period not less than 120 days.
- Video surveillance will not be disclosed by the corporation without written consent from the Chief Security Officer, court-ordered, or disclosure required by law.

Alarm Standards:

- Alarms will be installed in N.E.W.A. premises for fire detection and physical access.
- Fire alarms will be installed on all floors and in all rooms in accordance with local building codes.
- Physical access alarms will be installed on all doors, windows, or other access points into N.E.W.A. premises and controlled spaces within the premises.
- All alarms will be monitored by physical security personnel and linked to local fire and police as appropriate.
- Each controlled area will also include a manual activation for the alarm in case an intrusion is detected.

Member Awareness Practices:

- All Members will be briefed and provided a copy of all physical security policies upon hire, annually, and in the event of any changes to policies.
- Each Member will be given policies tailored to the area of access within the N.E.W.A. premises.
- Any Member found to be violating physical security policies will be subject to administrative discipline up to dismissal from the company as deemed necessary by the management team.

- All Members are directed to report security violation immediately to the physical security office and their direct supervisor.
- Physical security is the responsibility or all Members to help maintain a safe work environment for all personnel.

Section 3: Email Policy Standards

- Email policies regarding N.E.W.A. email will be defined as use of email, email forwarding, and email back up procedures. Access to N.E.W.A. email will follow the policies in place for Access Control.

Email Practices:

- N.E.W.A. email is for use for official company business and is not for personal correspondences.
- N.E.W.A. emails are subject to monitoring by the IT security team without notification to the user.
- N.E.W.A. emails will be deactivated after 30 days of inactivity.
- N.E.W.A. emails will be deleted after 45 days of inactivity.
- Data from N.E.W.A. emails will be maintained for a period of 3 years or in accordance with state and federal laws.
- All N.E.W.A. emails will contain a signature block from the sender containing, at a minimum, the full name, title, phone number, email address, work location, and the email disclaimer provided by the IT department (*This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee*

you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and deleted this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.).

- All N.E.W.A. emails will also include a digital signature generated by the IT department unique to the individual.

Email Forwarding Standards:

- Members must exercise the utmost caution when forwarding any email form inside or outside the corporation. Sensitive information must not be forwarded unless that email is absolutely necessary to N.E.W.A. business.
- Any N.E.W.A. email being forwarded outside of the company must also be copied (CC) to the individual's direct supervisor for tracking and accountability.

Email Back Up Standards:

- Email residing on the N.E.W.A. email servers will be backed up and retained for a period of no less than six weeks and can be recovered by request of the sender if needed.
- An email will be recovered in emergency recovery procedures within in the six week retention period.
- Email may be locally archived by the user on the N.E.W.A. file server. Locally archived emails will not be the responsibility of the IT department for recovery purposes.
- Emails may be printed for local retention by the users but must be safeguarded in the same manner as the email itself.

Section 4: Breach Reporting Responsibilities Standards and Practices

- It is the responsibility of all Members, temporary Members, and contracted Members to report data breaches immediately to the IT Security department.
- These breaches include, but are not limited to, data loss or disclosure, unauthorized systems access, the disclosure of N.E.W.A. data or PII.
- Data security breaches will be handled by the IT Emergency Breach Response Team in accordance with the N.E.W.A. Breach Response Policy.

Section 5: Mobile Policy and BYOD (Bring Your Own Device) Standards

- This section will outline the N.E.W.A. guidelines of use of mobile devices and BYOD within N.E.W.A. premises.

Mobile Device Practices:

- Members are directed to not use their personal mobile devices while on company time. The corporation does recognize that all Members have personal emergencies or personal items that need to be taken care of. Supervisors will make case by case exceptions for individual Members as need for these situations. It is recommended that personal situation accommodated for be taken care of outside of N.E.W.A. premises as to not interfere with other individuals work.
- Personal mobile devices should be turned off and put away in a safe place while at work. The corporation will take no responsibility for lost or stolen mobile devices.
- N.E.W.A. mobile devices are the responsibility of the assigned user and must be retained by that user at all times.

- N.E.W.A. mobile devices are not to be used for personal business and any personal phone calls or data usage will be the financial responsibility of the assigned user as outlined in the Mobile Device User Policies.

Bring Your Own Device (BYOD) Standards:

- Members that have a user agreement for BYOD will conduct N.E.W.A. business on these devices the same N.E.W.A. devices.
- The security and procedures for a BYOD will adhere to N.E.W.A. polices in regards to all N.E.W.A. related items.
- BYOD items are the sole responsibility of the individual and the corporation accepts no liability for damage, loss, licensing, support, or other issues that arise with the device.
- N.E.W.A. IT will provide support on BYOD only to functions that directly related to the individuals work needs.