Nuevo Mortgage Solutions Security Policy

Samuel E Barrionuevo

Trevecca Nazarene University

ITI-4070-01: Network Security/Cryptography

Dr. Kendrix

10th March 2023

Overview

Mortgage finance is a high-risk industry where companies deal with the livelihoods of their clients. Network security is paramount to protect sensitive data and adherence to best practices is essential for organizations to survive in wake of increasing attacks. This is crucial for successful business in the growing mortgage industry. As companies rapidly digitize data and communications, securing the personal information of individuals establishes trust and integrity. The intention for publishing this document is to protect client and employee information and to display commitment to protecting against the law and security incidents. The security team of Nuevo Mortgage Solutions seeks to involve all individuals and entities that deal with data and data systems. It is vital that all users understand and act according to this policy. Nuevo Mortgage Solutions is deeply committed to protecting all customer information, financial data, and company assets.

Introduction and Purpose

The purpose of this document is to list actionable security measures and policies for all users of computer equipment and systems. This is vital to the integrity of the company and all employees. This safeguards against unauthorized access, data, breaches, and network threats. Acting inappropriately can lead to cyberattacks, the compromise of data, legal ramifications, and loss of business. This document covers the computers, hardware, software, and facility components of Nuevo Mortgage Solutions. This includes personal devices, removable storage, and all network equipment. Anyone who has access to and utilizes company resources is considered a user and is expected to always conduct themselves appropriately. This document seeks not to impose user productivity and freedom, but rather to protect users and all involved parties against network security incidents.

Acceptable Use Policy

The Acceptable Use Policy covers all company computers, hardware, software, and removable storage devices of Nuevo Mortgage Solutions. A user is defined as anyone that has access to company devices or data whether an employee or third-party entity. All users are responsible for using company resources appropriately in accordance with all policies, procedures, standards, and applicable laws. The Acceptable Use Policy outlines acceptable user behavior and use of company resources. All employees and activity will be monitored when using Nuevo Mortgage Solutions resources.

Acceptable Use

Users may access, share, and use Nuevo Mortgage Solutions resources and information to fulfill permitted activities to fulfill job responsibilities. This includes accessing applications, completing work-related tasks, and communicating through business tunnels. In all cases are users responsible for reporting theft, loss, or unauthorized access of company data and devices. Authorized individuals within Nuevo Mortgage Solutions are allowed to monitor equipment, systems, traffic, and networks at any time to ensure compliance. Individual departments of Nuevo Mortgage Solutions are responsible for creating personal use guidelines, in all cases employees are expected to exercise good judgement for personal use and can refer to their supervisors if unsure. Personal use during break time and lunch times will be allotted by each department and managed by network managers. All devices are required to be secured with a password-protected lock screen that is visible when the device is unattended. Passwords must be compliant with the Access Control Policy. Any case of suspicious activity should be reported to security staff to ensure the safety of company customers, data, and employees.

Unacceptable Use

This outlines unacceptable behavior and use of company resources. All employees are strictly prohibited from engaging in illegal activities. This includes activities that could be considered unethical or a violation of rights. Intentionally introducing spam, malware, and viruses is prohibited. The violation of copyright laws through material and intellectual property is disallowed. Viewing and downloading objectionable content, using company equipment for personal business, and tampering with company software will result in violations of the Acceptable Use Policy. Intentionally revealing account or company information to others is strictly prohibited. Individuals are forbidden from engaging in or assisting the circumvention of company security. Activities that permit unauthorized access or use of Nuevo Mortgage Solutions resources are prohibited.

Access Control Policy

The Access Control Policy applies to all users and employees who have user accounts that have physical and logical access to company resources. The purpose of this policy is to defend sensitive information regarding employees and customers of Nuevo Mortgage Solutions.

Authority and Control Models

The chief security officer has ultimate authority over the Access Control Policy and the distribution of access and account privileges. The principle of least privilege and the separation of duties will be applied to all user accounts allowing them to have access to critical resources to fulfill all job duties. All user accounts will be given specific roles based on job requirements, responsibilities, and seniority. Both temporary and permanent access is managed by the CSO, and privileges are revoked after an access period elapses. Daily event logging and monthly audit schedules will contribute to account management and user accountability.

Credential and Access

All users with accounts are required to have strong passwords that contain more than ten characters that contain a capital letter, special character, and a number. These must be changed every six months and are not allowed to give their account information to other users or outsiders to store their information in a secure manner. Physical access to facilities requires a company identification card or token and all accounts are required to be backed by multi-factor authentication. Remote access users must use secure VPN tunnels through CATO VPN for secure private and internet access. Users are not permitted to access resources unauthorized.

Device Protection Policy

The purpose of the Nuevo Mortgage Solutions Device Protection Policy is to protect company assets and ensure the security of devices in the organization. This includes computers, firewalls, IDPS systems, routers, and other network hardware and Nuevo Mortgage Solutions devices. All devices are to be configured and managed by the network administrator, this includes installation, configuration, and management. All network devices will be configured to only operate on essential ports with traffic filters through access control lists with consistent monitoring. Between network segments will be active firewalls and IDPS systems to minimize risks and secure critical data centers. All devices are required to be up to date with the latest updates and patches. This will be done by the network administrator for company devices and update information will be released to employees with individual devices belonging to Nuevo Mortgage Solutions Additionally, antivirus and VPN software must be installed and run on all devices to secure online sessions and prevent the introduction of viruses and malware. This will be analyzed and monitored daily. Physical access to company networking devices such as routers, firewalls, and servers is restricted unless it is included in job responsibilities. Devices belonging to or leased by employees of Nuevo Mortgage Solutions must use company networks

or tunnels through CATO VPN, all other connections or connection sharing are strictly prohibited. Regular vulnerability assessments will be run on all devices, networks, and systems to protect company assets, employees, and customer information. Employees are prohibited from tampering with Nuevo Mortgage Solutions devices, settings, and connections without the permission of the network administrator.

Data Encryption Policy

The purpose of the Data Encryption policy is to ensure that all data is transferred in a safe and secure manner. This applies to all Nuevo Mortgage Solutions systems and devices that communicate on internal and external networks. Encrypting all data is a significant way to provide confidentiality, data integrity, and information privacy. All customer and Nuevo Mortgage Solutions data will be classified and secured based on security, the levels being public, private, and restricted. All data at rest will be encrypted using AES with a minimum key length of 256 bits including full disk encryption on devices. Additionally, all data in transit will be encrypted using TLS/SSL. All services with encryption options will use integrated encryption as well as limited visited websites to ones with strong encryption practices. All keys will be managed separately from transmitted data to ensure data security and verification functions will be authenticated with hashing practices.

Employee Roles and Training Policy

The purpose of all company policies is to ensure that both the behavior of employees can be influenced positively with the promotion of safety, integrity, trust, and transparency. This makes employee and management cooperation and input vital. This policy lists ways all Nuevo Mortgage Solutions members are trained, involved, and updated on company security information. All employees will be given daily emails and updates on company security, policy

revisions, and other policy changes to list security benefits. Every 6 months, employees will be required to complete remote security awareness training modules that pertain to company, network, and information security. New employees will be required to do this training as a part of onboarding additionally. Incident reporting and management will be made available to employees through reporting functions on company webpages, company email portals, and other company resources. All policy revisions and amendments are under the authority of the CSO, though reporting pitfalls and adjustments can be sent to the email address NMS.amendments@gmail.com. These suggestions and reports will be read and appraised.

Violations and Penalties

This policy outlines the consequences of violating any of the policies outlined in this document made by employees and third parties associated with Nuevo Mortgage Solutions. This is to ensure the safety of employees and customers of Nuevo Mortgage Solutions and outline the consequences of noncompliance to ultimately deter employees from compromising the security of Nuevo Mortgage Solutions. The penalty for noncompliance is based on the seriousness of the violation and the nature of the security compromise. Mild penalties can range from verbal or written warnings, training, and suspension of privileges. More serious penalties can lead to further disciplinary action such as termination of employment and even legal action and prosecution related to security breaches. Investigations for appropriate violation cases include interviews of relevant employees and customers, steps taken to assess violation severity, and the involvement of appropriate stakeholders to ensure compliance and proper punishment. Opportunities to appeal for disciplinary action involve proper evidence and an unbiased committee.