Nation One Mortgage Corporation
Device and User Terms of Use Policy
Effective Date: 3/14/2025

1. Purpose

This **Terms of Use Policy** outlines the requirements for all employees, contractors, and authorized users when accessing company-managed devices and services through Microsoft Entra. The policy ensures compliance with security, confidentiality, and operational standards while maintaining the integrity of Nation One Mortgage Corporation’s IT environment.

2. Scope

This policy applies to:

- All employees, contractors, and third-party vendors accessing Microsoft Entra and associated services.
- All company-issued and personal devices used for work-related activities.
- Any system, data, or application accessed through company credentials.

3. Device Usage Requirements

All devices, whether company-owned or personal, used to access Microsoft Entra services must:

1. **Be Enrolled in Endpoint Management**: Devices must be registered and compliant with Intune policies.
2. **Meet Security Requirements**:
    - Up-to-date operating system and security patches.
    - Active and approved antivirus software.
    - Full-disk encryption enabled where applicable.
3. **Be Used for Authorized Purposes**: Personal use of company devices should not interfere with business operations. Personal devices used for company business must adhere to security policies.
4. **Enable Multi-Factor Authentication (MFA)**: MFA is required for all logins to company systems.
5. **Prohibit Unauthorized Software**: Users shall not install or run unauthorized applications that pose security risks.

4. User Access and Authentication

Users must:

- Use only assigned credentials and not share login information with others.
- Notify IT immediately if credentials are compromised.
- Use strong passwords that meet company standards.
- Log out or lock devices when unattended.

5. Data Protection and Confidentiality

Users must:

- Store and transfer company data only through approved applications and services.
- Refrain from storing sensitive or customer information on unauthorized devices.
- Report data breaches or security incidents to IT immediately.

6. Prohibited Activities

The following activities are strictly prohibited:

- Bypassing security controls, including unauthorized VPNs or proxy servers.
- Accessing or distributing illegal, offensive, or inappropriate content.
- Using company devices or credentials for personal gain or non-work-related commercial purposes.
- Modifying system configurations without IT authorization.

7. Compliance and Enforcement

- Failure to comply with this policy may result in disciplinary action, including revocation of access, suspension, or termination of employment.
- IT reserves the right to monitor, audit, and take necessary actions to ensure compliance.
- Policy violations may be reported to law enforcement if necessary.

8. Policy Updates

This policy may be updated periodically. Users will be notified of changes and must review and acknowledge updates as required.

Acknowledgment By accessing Microsoft Entra and company devices, you acknowledge that you have read, understood, and agree to abide by this policy.

For questions or concerns, please contact: 856-334-1200