INTERNAL POLICY DOCUMENT Hyperbolic Mortgage

Policy Name: Data Security & Acceptable Use Policy
Version: 3.1
Effective Date: February 1, 2025
Approved By: Chief Information Security Officer (CISO)
Document Type: Internal Policy

1. Purpose
This policy establishes the standards for responsible use and protection of company systems, data, and technology resources. It applies to all employees, contractors, and third parties who access Hyperbolic Mortgage information assets.

2. Scope
This policy covers:
• Workstations, laptops, mobile devices
• Company email and communication systems
• Customer financial data and confidential information
• Cloud and on■prem applications
• Third■party SaaS platforms used for business operations

3. Acceptable Use Requirements
Employees must:
• Use company systems only for approved business activities
• Protect confidential borrower and operational data
• Maintain strong passwords and enable MFA on all accounts
• Store files only in approved systems (OneDrive, company SharePoint)

Employees must not:
• Email customer financial data to personal accounts
• Upload sensitive documents into unauthorized AI or public apps
• Connect unapproved USB devices to company machines
• Share internal documents outside the organization without authorization

4. Data Handling Standards
• All borrower documents must be stored in secure, access■controlled systems
• PHI, PII, and financial records must be encrypted at rest and in transit
• Sensitive files must not be stored locally unless explicitly required
• External sharing requires manager and Security approval

5. Incident Reporting
All security incidents—including lost devices, suspected phishing, unauthorized access, or data exposure—must be reported immediately to Security Operations via security@hyperbolicmortgage.com.

6. Enforcement
Violations of this policy may result in disciplinary action up to and including termination, as well as potential legal consequences. Compliance is mandatory for continued access to corporate systems.

7. Review & Updates

This policy is reviewed annually by the Security, Legal, and Compliance teams and updated based on regulatory and operational requirements.

Internal Use Only — Not for Public Distribution.