Blossom Banking: Cyber-Security Protocol 2026

1.1 Multi-Factor Authentication (MFA) Requirements

All Blossom Banking users must enroll in MFA. We support three methods: 1. Blossom Token App (preferred). 2. SMS Gateway (not recommended for high-limit accounts). 3. Hardware Security Keys (YubiKey). Codes generated by the app expire every 30 seconds. If a user enters an expired code 5 times, the MFA service will suspend the account for 1 hour.

2.1 Advanced Password Entropy Standards

Passwords must meet a minimum entropy score of 60 bits. Requirements: - Minimum 12 characters, maximum 128 characters.

- Must include characters from at least three of these groups: Latin uppercase, Latin lowercase, digits (0-9), and non-alphanumeric symbols (!, $, #, %).

- Passwords cannot contain the user's date of birth or social security number digits.

- Passwords expire every 180 days for standard users and every 60 days for administrators.

3.1 Trusted Device Management

When a user selects 'Remember this device', a persistent encrypted cookie is stored. This cookie is valid for exactly 30 days. After this period, MFA re-verification is mandatory. The system tracks the MAC address and IP geolocation. If a login attempt occurs from a distance greater than 500 miles from the last successful login, an 'Identity Alert' email is triggered.

4.1 Account Recovery Workflow

Step 1: User submits 'Forgot Username' request via the web portal.

Step 2: System sends a masked hint to the secondary email on file.

Step 3: If the hint is not enough, the user must provide the last 4 digits of their Blossom Debit Card and the ZIP code of their primary residence.

Step 4: Once identity is confirmed, the username is displayed on screen for 60 seconds.