Security Policy for the Spotify Data Breach:

Purpose

To protect Spotify user accounts and data by preventing unauthorized access, improving password security, and responding quickly to threats.

Key Security Goals

- **Confidentiality**: Only authorized users should access account details.
- **Integrity**: Account information should stay accurate and untampered.
- **Availability**: Users should access their accounts with minimal disruptions.

Security Measures

1. **Strong Password Requirements**
   - Require users to create strong, unique passwords (at least 8 characters, including letters, numbers, and symbols).
   - Regularly remind users of password security practices and encourage using unique passwords across platforms.
2. **Two-Factor Authentication (2FA)**
   - Offer 2FA to all users, adding a second security step to better protect accounts.
3. **Anomaly Detection and Rate Limiting**
   - Monitor for suspicious login patterns, like multiple failed login attempts.
   - Apply limits on repeated login attempts to block automated attacks.

Relation to the CIA Triad

- **Confidentiality**: Protects account access with strong passwords and 2FA.
- **Integrity**: Ensures account data stays accurate with detection of suspicious activity.
- **Availability**: Rate limiting and monitoring minimize makes the service readily available.