Security Requirements & Test Plan — Neural Implant System

A. Functional Security Requirements

- Device Identity & Attestation: Each device MUST have a unique device ID and device key pair stored in a secure element. On commissioning, device MUST perform attestation.
- Mutual Authentication: All channels MUST be mutually authenticated (mTLS or equivalent).
- Confidentiality & Integrity: All telemetry/control MUST use AEAD (ChaCha20-Poly1305 or AES-GCM) with sequence numbers and timestamps.
- Firmware Management: Devices MUST accept only cryptographically signed firmware with rollback protection.
- Least-Privilege Command Model: Partition command API; critical functions require multi-step authorization.
- Local Safety Interlocks: Hardware/software watchdogs and safe-mode on integrity violations.
- Logging & Auditing: Security events MUST be logged with tamper-evident records.
- Revocation & Key Rotation: Support revocation of device certs and rotation of signing keys.

B. Non-Functional Security Requirements

- Cryptographic Algorithms: Use Curve25519/X25519, Ed25519, SHA-256, ChaCha20-Poly1305.
- Key Storage: Private keys MUST reside in a secure element (ATECC, TPM, TrustZone).
- Resilience: System MUST tolerate transient network failures without loss of critical safety functions.
- Latency: Characterize worst-case latency for safety-critical commands.
- Updatability: OTA updates MUST be atomic and secure.
- Maintainability: CI/CD with reproducible builds and signed artifacts.

C. Verification & Validation (Test Plan)

- Penetration testing on firmware, comms stack, and backend prior to clinical trials.
- Fuzz testing of the command API and protocol.
- Third-party cryptographic audit for key management & attestation.
- Safety validation: simulate compromise scenarios on bench hardware to verify safe fallback behavior.
- Supply chain audit: supplier security questionnaires and component tests.
- Continuous monitoring: anomaly detection in telemetry and automated alerting.