Firestore Security Hardening — Phase 3 Summary Objective Re-establish full app functionality while preserving org-level data isolation and preparing for role-based access. Root Cause Summary Over-strict org validation prevented query reads. Missing custom claims caused authentication mismatches. Cross-collection references required integrity checks. Fix Overview Restored valid access patterns for authenticated users. Admins can write only within org boundaries. Added reference validation for campaign-linked docs. Explicit subcollection read-only rules included. Core Utility Functions function isSignedIn() { return request.auth != null; } function userOrg() { return request.auth.token.orgId; } function sameOrg(resource) { return isSignedIn() && resource.data.orgId == userOrg(); } Security Guarantees Achieved Per-org data isolation enforced. Cross-collection integrity maintained. Admin-only modification restored. Functional reads for signed-in users. Next Phase Phase 4: Role-based permissions (admin/coach/athlete/donor) UI updates to honor roles. Cloud Functions to automate claims.