# API Permission Testing for ZeigoWriterRole

## Test Case ID: API-SEC-001

### Test Objective:

To validate that the ZeigoWriterRole has appropriate API-level permissions (read-only access) when accessing cross-organization relationship data.

### Pre-conditions:

- ZeigoWriterRole user credentials are available  
- Test environment with Knowledge Graph API is accessible  
- Sample organization relationship data exists in the system

### Test Data:

- User with ZeigoWriterRole permissions  
- Sponsor Organization ID: {sponsorId}  
- Supplier Organization ID: {supplierId}  
- Existing Relationship ID: {relationshipId}  
- Sample JSON payload for creation/modification attempts

### API Permission Tests:

1. GET Requests (Read Operations)

- Expected: HTTP 200 OK responses  
- Test these endpoints:  
 • GET /api/organizations/{sponsorId}/relationships  
 • GET /api/organizations/{supplierId}/relationships  
 • GET /api/relationships/{relationshipId}  
- Verification points:  
 • Response contains complete relationship data  
 • All expected fields are present and accessible  
 • Response times are within acceptable limits

2. POST Requests (Create Operations)

- Expected: HTTP 403 Forbidden  
- Test these endpoints:  
 • POST /api/relationships  
 • POST /api/organizations/{sponsorId}/relationships  
- Request body example:  
 {  
 "type": "supplier\_to\_sponsor",  
 "sourceOrganizationId": "{supplierId}",  
 "targetOrganizationId": "{sponsorId}",  
 "status": "active"  
 }  
- Verification points:  
 • Response includes clear permission error message  
 • Error message specifically mentions write/create permission lacking  
 • No relationship is created (verify with GET request)

3. PUT Requests (Full Update Operations)

- Expected: HTTP 403 Forbidden  
- Test these endpoints:  
 • PUT /api/relationships/{relationshipId}  
- Request body example:  
 {  
 "type": "supplier\_to\_sponsor",  
 "status": "inactive",  
 "metadata": {  
 "lastUpdated": "2023-05-15T10:30:00Z"  
 }  
 }  
- Verification points:  
 • Response includes permission-related error message  
 • No data is updated (verify with subsequent GET)  
 • Error format is consistent with API error standards

4. PATCH Requests (Partial Update Operations)

- Expected: HTTP 403 Forbidden  
- Test these endpoints:  
 • PATCH /api/relationships/{relationshipId}  
 • PATCH /api/organizations/{sponsorId}/relationships/{relationshipId}  
- Request body example:  
 {  
 "status": "inactive"  
 }  
- Verification points:  
 • Response includes permission-related error message  
 • No fields are updated (verify with subsequent GET)  
 • Error message clearly indicates which operation was rejected

5. DELETE Requests (Delete Operations)

- Expected: HTTP 403 Forbidden  
- Test these endpoints:  
 • DELETE /api/relationships/{relationshipId}  
 • DELETE /api/organizations/{sponsorId}/relationships/{relationshipId}  
- Verification points:  
 • Response includes permission-related error message  
 • Relationship data remains intact (verify with subsequent GET)  
 • System logs record the unauthorized delete attempt

6. Error Response Format Verification

For all 403 responses, verify that:  
- The response follows the standard API error format  
- The error message is specific to the ZeigoWriterRole permissions  
- No sensitive information is exposed in error messages  
- The Content-Type header is appropriately set  
- Response times for error cases are within acceptable limits

### Important Note:

The appropriate status code for permission issues should be 403 Forbidden rather than 400 Bad Request. A 400 status indicates a malformed request, while 403 specifically indicates that the authentication was successful but the authenticated user doesn't have the right permissions for the requested operation.

### Test Results:

1. GET Operations: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
2. POST Operations: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
3. PUT Operations: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
4. PATCH Operations: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
5. DELETE Operations: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
6. Error Format Validation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Overall Test Result: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### Execution Notes:

This test case is designed to be executed once API endpoints are available. Testing can be performed manually using tools like Postman or implemented as automated API tests using a framework such as RestAssured, Supertest, or other HTTP client libraries.

Estimated Test Execution Time: 1-2 hours (manual testing)