

# Bài Kiểm Tra Node.js

---

## 0. Yêu Cầu Chuẩn Bị

- Tải Repository mẫu này về máy tính và thực hiện bài kiểm tra trên chính source code này.
  - Nộp bài: Đẩy code lên GitHub repository cá nhân (**public**) và gửi link qua Google Classroom. Không commit sau khi nộp.
  - Được tra cứu tài liệu chính thức của Express, Swagger, JWT, bcryptjs, Zod.
  - **Tắt tất cả extension AI** (Tabnine, GitHub Copilot, Codeium, BlackBoxAI, v.v.).
  - Thời gian: **150 phút**.
  - Tích hợp **Swagger** để test API.
- 

## 1. Xây Dựng Models (1 điểm)

### 1.1. User (0.5 điểm)

- **email**: String, required, unique
- **username**: String, required, unique
- **password**: String, required
- **role**: String, default `member`, enum [`member`, `admin`, `superAdmin`]
- **createdAt**: Date, default `Date.now`
- **courses**: Array of ObjectId, ref Course (khóa học người dùng tạo)
- **coursesRegistered**: Array of ObjectId, ref Course (khóa học đã đăng ký)

### 1.2. Course (0.5 điểm)

- **title**: String, required
  - **description**: String, required
  - **content**: String, required
  - **createdAt**: Date, default `Date.now`
  - **students**: Array of ObjectId, ref User
  - **price**: Number, default 0
  - **isArchived**: Boolean, default `false` (để đánh dấu khóa học đã lưu trữ hoặc ngừng kinh doanh)
- 

## 2. Thao Tác Khách (Guest Actions) (2 điểm)

### 2.1. Đăng Ký (0.5 điểm)

- **Endpoint**: `POST /api/auth/register`
- **Body**: email, username, password (min 6 ký tự), role mặc định là `member`
- Hash password bằng `bcryptjs`.
- **Response**: `{ status: "success", data: { user: { email, username, role } } }`
- **Validation**: Sử dụng `zod`.

### 2.2. Đăng Nhập (0.5 điểm)

- **Endpoint:** `POST /api/auth/login`
- **Body:** email, password
- **Response:** `{ status: "success", data: { user: { email, username, role }, token } }`, token expires in 30 days.
- **Validation:** Sử dụng `zod`.

### 2.3. Danh Sách Khóa Học (0.5 điểm)

- **Endpoint:** `GET /api/courses`
- **Response:** `{ status: "success", data: [courses] }`
- Khóa học đã lưu trữ sẽ không được trả về.

### 2.4. Chi Tiết Khóa Học (0.5 điểm)

- **Endpoint:** `GET /api/courses/:id`
- **Response:** `{ status: "success", data: course }`
- **404:** `{ status: "error", message: "Course not found" }`
- **Lỗi:** Nếu khóa học đã lưu trữ, trả về lỗi 404.

---

## 3. Middleware Xác Thực & Phân Quyền (1 điểm)

- **verifyUser:** Xác thực token JWT (dùng `jwt.js`), gắn user vào `req.user`.
- **restrictTo:** Kiểm tra `req.user.role` (`admin` hoặc `superAdmin`) cho các endpoint POST, PATCH, DELETE của Course.

---

## 4. Thao Tác Người Dùng đã đăng nhập (1.5 điểm)

### 4.1. Đăng Ký Khóa Học (0.5 điểm)

- **Endpoint:** `POST /api/courses/register/:id`
- **Header:** Authorization Bearer Token
- **Response:** `{ status: "success", data: course }`
- **Lỗi khi gặp các trường hợp sau:**
  - Đã đăng ký hoặc khóa học đó rồi.
  - Khóa học không tồn tại.
  - Khóa học đã lưu trữ.

### 4.2. Danh Sách Khóa Học Đã Đăng Ký (0.5 điểm)

- **Endpoint:** `GET /api/courses/registered`
- **Header:** Authorization Token
- **Response:** `{ status: "success", data: [courses] }`
- **Lỗi:** Chưa đăng nhập.

### 4.3. Hủy Đăng Ký Khóa Học (0.5 điểm)

- **Endpoint:** `DELETE /api/courses/register/:id`
- **Header:** Authorization Token

- **Response:** { status: "success", data: course }
  - **Lỗi:** Chưa đăng ký khoá học hoặc khóa học không tồn tại.
- 

## 5. Thao Tác Admin và SuperAdmin (2.5 điểm)

### 5.1. Tạo Khóa Học (0.5 điểm)

- **Endpoint:** POST /api/courses
- **Header:** Authorization Bearer Token (admin, superAdmin)
- **Body:** title, description, content
- **Response:** { status: "success", data: course }
- **Lỗi:** Thiếu trường hoặc không có quyền.

### 5.2. Cập Nhật Khóa Học (0.5 điểm)

- **Endpoint:** PATCH /api/courses/:id
- **Header:** Authorization Bearer Token (admin, superAdmin)
- **Body:** title, description, content (optional)
- **Response:** { status: "success", data: course }
- **Lỗi:** Khóa học không tồn tại hoặc không đủ quyền.

### 5.3. Xóa Khóa Học (0.5 điểm)

- **Endpoint:** DELETE /api/courses/:id
- **Header:** Authorization Bearer Token (admin, superAdmin)
- **Response:** { status: "success", data: course }
- **Lỗi khi gặp một trong số trường hợp sau:**
  - Khóa học không tồn tại.
  - Không đủ quyền.
  - Khóa học đã có người đăng ký.

### 5.4. Lưu trữ khóa học (0.5 điểm)

- **Endpoint:** DELETE /api/courses/archive/:id
- **Header:** Authorization Bearer Token (admin, superAdmin)
- **Response:** { status: "success", data: course }
- **Lỗi khi gặp một trong số trường hợp sau:**
  - Khóa học không tồn tại.
  - Không đủ quyền.
  - Khóa học đã có người đăng ký.

### 5.5. Bỏ lưu trữ khóa học (0.5 điểm)

- **Endpoint:** PATCH /api/courses/restore/:id
- **Header:** Authorization Bearer Token (admin, superAdmin)
- **Response:** { status: "success", data: course }
- **Lỗi khi gặp một trong số trường hợp sau:**
  - Khóa học không tồn tại.

- Không đủ quyền.
- Khóa học chưa được lưu trữ.

---

## 6. Thao Tác SuperAdmin (2 điểm)

Những thao tác sau đây chỉ dành cho người dùng có role **superAdmin**.

### 6.1. Danh Sách Người Dùng (0.5 điểm)

- **Endpoint:** **GET /api/users**
- **Header:** Authorization Token (superAdmin)
- **Response:** **{ status: "success", data: [users] }**
- Không trả về người dùng có role **superAdmin**.

### 6.2. Khóa Người Dùng (0.5 điểm)

- **Endpoint:** **PATCH /api/users/block/:id**
- **Header:** Authorization Token (superAdmin)
- **Response:** **{ status: "success", data: user }**
- **Lỗi:** Người dùng không tồn tại hoặc đã bị khóa.

### 6.3. Mở Khóa Người Dùng (0.5 điểm)

- **Endpoint:** **PATCH /api/users/unblock/:id**
- **Header:** Authorization Token (superAdmin)
- **Response:** **{ status: "success", data: user }**
- **Lỗi:** Người dùng không tồn tại hoặc chưa bị khóa.

### 6.4. Bổ nhiệm admin (0.5 điểm)

- **Endpoint:** **PATCH /api/users/appoint-admin/:id**
- **Header:** Authorization Token (superAdmin)
- **Response:** **{ status: "success", data: user }**
- **Lỗi:** Người dùng không tồn tại hoặc đã là admin.

---

## Cách Tính Điểm

1. **Models:** 1 điểm
  - User: 0.5 điểm
  - Course: 0.5 điểm
2. **Thao Tác Khách (chưa đăng nhập):** 2 điểm
  - Đăng ký: 0.5 điểm
  - Đăng nhập: 0.5 điểm
  - Danh sách khóa học: 0.5 điểm
  - Chi tiết khóa học: 0.5 điểm
3. **Middleware Xác Thực & Phân Quyền:** 1 điểm
4. **Thao Tác Người Dùng đã đăng nhập:** 1.5 điểm
  - Đăng ký khóa học: 0.5 điểm

- Danh sách khóa học đã đăng ký: 0.5 điểm
- Hủy đăng ký khóa học: 0.5 điểm

**5. Thao Tác Admin và SuperAdmin: 2.5 điểm**

- Tạo khóa học: 0.5 điểm
- Cập nhật khóa học: 0.5 điểm
- Xóa khóa học: 0.5 điểm
- Lưu trữ khóa học: 0.5 điểm
- Bỏ lưu trữ khóa học: 0.5 điểm

**6. Thao Tác SuperAdmin: 2 điểm**

- Danh sách người dùng: 0.5 điểm
- Khóa người dùng: 0.5 điểm
- Mở khóa người dùng: 0.5 điểm
- Bổ nhiệm admin: 0.5 điểm

**Trừ Điểm**

- Lỗi logic (role, validation, status code, message): trừ 0.25 điểm/lỗi.
- Thiếu Swagger hoặc tài liệu không chính xác: trừ 0.5 điểm.

**Hết.**