🔒 NÂNG CẤP BẢO MẬT DASHBOARD PHẢN BIỆN VIÊN

Ngày triển khai: 08/11/2025
Mục tiêu: Xây dựng chức năng hiển thị nội dung bài báo trong dashboard phản biện với bảo mật tuyệt đối theo cơ chế **double-blind review** đáp ứng yêu cầu quân sự.

📋 TÓM TẮT CÁC THAY ĐỔI

1. ✅ Ẩn danh tuyệt đối thông tin tác giả (Double-Blind Review)

File: `app/dashboard/reviewer/review/[id]/page.tsx`

Thay đổi:
- ❌ Loại bỏ hoàn toàn thông tin `author` khỏi Prisma query
- ❌ Không hiển thị tên tác giả và đơn vị trong UI
- ✅ Thay thế bằng "[Ẩn danh theo nguyên tắc phản biện kín]"

Bảo mật đạt được:
- Reviewer không thể biết ai là tác giả bài báo
- Tuân thủ nghiêm ngặt nguyên tắc double-blind review

---

2. ✅ Tăng cường bảo mật API truy cập file

File: `app/api/files/[id]/route.ts`

Cải tiến chính:

a) Kiểm tra quyền truy cập nâng cao

```
// Thêm kiểm tra reviewer được gán
const isAssignedReviewer = file.submission?.reviews?.some(
  review => review.reviewerId === session.uid
) || false;
```

b) Token tạm thời với thời gian ngắn

```
// Reviewer: 15 phút
// Admin/Author: 1 giờ
const expiryTime = isAssignedReviewer && !isAdmin ? 900 : 3600;
```

c) Ẩn thông tin tác giả trong API response

```
// Với reviewer, chỉ trả về id và code, không có createdBy
submission: isAssignedReviewer && !isAdmin ? {
  id: file.submission?.id,
  code: file.submission?.code
} : file.submission
```

Bảo mật đạt được:
- Chỉ reviewer được gán mới truy cập được file
- URL hết hạn sau 15 phút (tránh chia sẻ)
- Không thể đoán biết thông tin tác giả từ API

---

3. ✅ Audit Logging chi tiết

File: `lib/audit-logger.ts` + `app/api/files/[id]/route.ts`

Thêm event types:

```
FILE_ACCESSED = 'FILE_ACCESSED',
FILE_ACCESS_DENIED = 'FILE_ACCESS_DENIED',
FILE_DELETE = 'FILE_DELETE',
```

Ghi log:
- ✅ Mọi lần truy cập file (thành công)
- ✅ Mọi lần bị từ chối truy cập (thất bại)
- ✅ Lưu thông tin: userId, IP, submission code, access type, expiry time

Bảo mật đạt được:
- Theo dõi toàn bộ hoạt động truy cập file
- Phát hiện hành vi bất thường
- Tuân thủ TT41 về nhật ký hệ thống

---

4. ✅ Watermark cảnh báo bảo mật

File: `app/dashboard/reviewer/review/[id]/pdf-viewer-client.tsx`

Thêm banner cảnh báo:

```
⚠️ TÀI LIỆU TUYỆT MẬT - PHẢN BIỆN KHOA HỌC

• Cấm sao chép, phát tán tài liệu này dưới mọi hình thức
• Tài liệu chỉ dùng cho mục đích phản biện khoa học
• Thông tin tác giả đã được ẩn danh theo nguyên tắc double-blind
• Mọi hành vi vi phạm sẽ bị ghi lại và xử lý nghiêm khắc
• Link xem có hiệu lực 15 phút và được ghi log truy cập
```

Bảo mật đạt được:
- Nhắc nhở reviewer về tính bảo mật

- Răn đe vi phạm
- Tăng nhận thức an ninh thông tin

🎯 KẾT QUẢ ĐẠT ĐƯỢC

Về mặt học thuật:

✅ Reviewer có thể xem toàn bộ nội dung bài báo (PDF)
✅ Giao diện phản biện đầy đủ, chuyên nghiệp
✅ Không ảnh hưởng đến quy trình phản biện

Về mặt bảo mật:

🔒 **Double-blind review tuyệt đối:** Reviewer không biết tác giả
🔒 **Quyền truy cập nghiêm ngặt:** Chỉ reviewer được gán
🔒 **Token tạm thời:** 15 phút hết hạn
🔒 **Audit trail đầy đủ:** Ghi log mọi truy cập
🔒 **Cảnh báo rõ ràng:** Watermark bảo mật

Tuân thủ:

✅ Nguyên tắc double-blind review quốc tế
✅ Quy định bảo mật quân sự
✅ Thông tư 41/2022/TT-BTTTT về nhật ký hệ thống

📝 HƯỚNG DẪN SỬ DỤNG

Cho Reviewer:

1. Đăng nhập vào hệ thống
2. Vào **Dashboard Reviewer → Phản biện của tôi**
3. Click vào bài báo cần phản biện
4. Đọc nội dung bài báo trực tiếp trên trang (PDF viewer)
5. Điền biểu mẫu phản biện
6. Nộp phản biện

Lưu ý:
- ❌ Không biết tên tác giả (ẩn danh)
- ⏰ Link xem PDF chỉ có hiệu lực 15 phút
- 📝 Mọi thao tác được ghi log

Cho Admin/Editor:

- Có thể xem thông tin tác giả
- Link xem PDF có hiệu lực 1 giờ
- Có quyền truy cập vào audit logs

🔧 KỸ THUẬT TRIỂN KHAI

Stack:

- Next.js 14.2.28 (App Router)
- Prisma ORM
- AWS S3 (Signed URLs)
- JWT Authentication
- PostgreSQL

Các file đã sửa:

1. `app/dashboard/reviewer/review/[id]/page.tsx` - Ẩn tác giả
2. `app/api/files/[id]/route.ts` - Bảo mật API
3. `lib/audit-logger.ts` - Thêm event types
4. `app/dashboard/reviewer/review/[id]/pdf-viewer-client.tsx` - Watermark

Build Status:

✅ TypeScript compilation: PASSED
✅ Next.js build: PASSED
✅ All type checks: PASSED

📊 SO SÁNH TRƯỚC/SAU

Tiêu chí	Trước	Sau
Thông tin tác giả	❌ Hiển thị đầy đủ	✅ Ẩn hoàn toàn
Kiểm tra quyền reviewer	❌ Không có	✅ Kiểm tra nghiêm ngặt
Thời hạn token	⏰ 1 giờ	⏰ 15 phút (reviewer)
Audit logging	📝 Cơ bản	✅ Chi tiết đầy đủ
Cảnh báo bảo mật	❌ Không có	✅ Watermark rõ ràng
Double-blind review	❌ Vi phạm	✅ Tuân thủ 100%

✅ CHECKLIST BẢO MẬT

- [x] Ẩn thông tin tác giả khỏi reviewer
- [x] Kiểm tra quyền truy cập file
- [x] Token tạm thời (15 phút)
- [x] Ghi log mọi truy cập
- [x] Watermark cảnh báo
- [x] Không có metadata nhạy cảm trong response

- [x] Tuân thủ double-blind review
- [x] Build và test thành công

🚀 TƯƠNG LAI

Có thể mở rộng:

1. Thêm watermark trực tiếp vào PDF (server-side)
2. Tích hợp DRM (Digital Rights Management)
3. Cảnh báo screenshot/print screen
4. Tự động blur nội dung khi inactive
5. Giới hạn số lần truy cập file

Kết luận: Hệ thống đã đạt mức bảo mật cao, tuân thủ nguyên tắc double-blind review và quy định bảo mật quân sự. Reviewer có thể làm việc hiệu quả mà không biết thông tin tác giả.