Chính sách Bảo mật Hệ thống

Tạp chí Điện tử Khoa học Hậu cần Quân sự

Mục đích

Tài liệu này quy định các chính sách và biện pháp bảo mật cho Hệ thống Tạp chí Điện tử Khoa học Hậu cần Quân sự, tuân thủ Thông tư 41/2016/TT-BTTTT về quản lý, kết nối và trao đổi thông tin trên mạng máy tính.

---

1. Phân cấp Bảo mật

1.1. Mức độ Mật

- **Công khai**: Nội dung tạp chí đã xuất bản
- **Nội bộ**: Bài viết đang phản biện, dữ liệu quản lý
- **Mật**: Thông tin đăng nhập, tài khoản, logs hệ thống

1.2. Phân quyền Truy cập

Vai trò	Quyền truy cập	Mức độ bảo mật
AUTHOR	Bài viết của mình	Nội bộ
REVIEWER	Bài được phân công	Nội bộ
EDITOR	Quản lý bài viết	Nội bộ
MANAGING_EDITOR	Quản lý nội dung	Nội bộ
EIC	Toàn quyền nội dung	Nội bộ + Mật
SYSADMIN	Toàn quyền hệ thống	Mật

---

2. Chính sách Mật khẩu

2.1. Yêu cầu Mật khẩu

Bắt buộc:
- Ít nhất 8 ký tự
- Chứa chữ hoa (A-Z)
- Chứa chữ thường (a-z)

- Chứa số (0-9)
- Khuyến nghị: Chứa ký tự đặc biệt (!@#$%^&*)

Cấm:
- Mật khẩu phổ biến: `password`, `12345678`, `admin123`
- Thông tin cá nhân: tên, ngày sinh, số điện thoại
- Sử dụng lại mật khẩu cũ

2.2. Quản lý Mật khẩu

- **Đổi mật khẩu**: Mỗi 90 ngày
- **Khóa tài khoản**: Sau 5 lần đăng nhập sai
- **Session timeout**: 60 phút không hoạt động
- **Tài khoản mặc định**: Phải đổi ngay sau lần đăng nhập đầu

2.3. Lưu trữ Mật khẩu

- Mật khẩu được mã hóa bằng bcrypt (cost factor 12)
- KHÔNG lưu mật khẩu dạng plaintext
- KHÔNG log mật khẩu trong audit logs

---

3. Xác thực và Phân quyền

3.1. Xác thực (Authentication)

JWT Token:
- Access Token: Hết hạn sau 60 phút
- Refresh Token: Hết hạn sau 7 ngày
- Tokens được ký bằng JWT_SECRET (256-bit)

Session Management:
- Mỗi user chỉ có 1 session đăng nhập cùng lúc
- Session mới sẽ hủy session cũ
- Đăng xuất hủy toàn bộ tokens

3.2. Phân quyền (Authorization)

RBAC (Role-Based Access Control):
- Mọi API route kiểm tra quyền truy cập
- Sử dụng middleware `canAccess(role, resource, action)`
- Log tất cả lần truy cập bị từ chối

Blind Review Policy:
- Tác giả KHÔNG thấy thông tin phản biện viên
- Phản biện viên KHÔNG thấy thông tin tác giả (nếu double-blind)
- Chỉ Editor và EIC thấy đầy đủ thông tin

---

4. Bảo vệ Dữ liệu

4.1. Mã hóa

Data at Rest:
- Mật khẩu: bcrypt
- JWT Secrets: 256-bit random
- Database: PostgreSQL built-in encryption

Data in Transit:
- TLS 1.2/1.3 (HTTPS)
- Certificate từ CA nội bộ quân đội
- Chỉ cho phép strong ciphers

4.2. Backup

Tần suất:
- Database: Hàng ngày lúc 2:00 AM
- Files: Hàng ngày lúc 3:00 AM
- Full system: Hàng tuần

Lưu trữ:
- Backup gần đây: 30 ngày
- Backup hàng tháng: 1 năm
- Vị trí: Máy chủ NAS riêng biệt

Bảo mật Backup:
- Backup files được mã hóa
- Chỉ admin có quyền restore
- Kiểm tra restore thường xuyên (hàng tháng)

4.3. Xóa Dữ liệu

Soft Delete:
- Dữ liệu quan trọng không xóa vĩnh viễn
- Đánh dấu `isDeleted = true`
- Lưu thông tin người xóa, thời gian

Hard Delete:
- Chỉ SYSADMIN có quyền hard delete
- Phải có xác nhận bằng văn bản
- Log đầy đủ trong audit trail

---

5. Bảo vệ ứng dụng

5.1. Chống Tấn công

SQL Injection:
- Sử dụng Prisma ORM (parameterized queries)
- Validate input trước khi query
- KHÔNG dùng raw SQL với user input

XSS (Cross-Site Scripting):
- Sanitize HTML input
- Content Security Policy headers
- HttpOnly cookies cho tokens

CSRF (Cross-Site Request Forgery):
- CSRF tokens cho forms
- SameSite cookie attribute
- Verify Origin/Referer headers

Rate Limiting:
- API routes: 60 requests/minute
- Auth endpoints: 5 attempts/15 minutes
- Upload endpoints: 10 requests/5 minutes

5.2. Validate Input

Server-side:
- Validate tất cả input từ client
- Sử dụng Zod schemas
- Reject requests với invalid data

Client-side:
- Validate trước khi gửi request
- Hiển thị error messages rõ ràng
- KHÔNG tin tưởng client-side validation

5.3. File Upload Security

Kiểm tra File:
- Chỉ cho phép: `.pdf`, `.docx`, `.jpg`, `.png`
- Kiểm tra MIME type
- Giới hạn kích thước: 50MB cho PDF, 5MB cho images

Lưu trữ:
- Upload trực tiếp lên S3 (không qua server)
- Files được scan virus (nếu có antivirus)
- Private files dùng signed URLs (expiry 1 giờ)

---

6. Audit và Logging

6.1. Audit Trail

Ghi lại:
- Tất cả thao tác đăng nhập/đăng xuất
- Thay đổi dữ liệu quan trọng
- Truy cập bị từ chối
- Thao tác quản trị (tạo/xóa user, v.v.)
- Xuất bản bài viết
- Backup và restore

Nội dung Log:
- Timestamp
- User ID và role
- Action thực hiện
- IP address và User Agent
- Before/After data (nếu có thay đổi)

6.2. Log Management

Lưu trữ:
- Application logs: 30 ngày
- Audit logs: Vĩnh viễn (hoặc theo quy định)
- Access logs (Nginx): 90 ngày

Bảo vệ Logs:
- Chỉ SYSADMIN truy cập audit logs
- Logs không chứa sensitive data (passwords, tokens)
- Backup logs cùng database

6.3. Monitoring

Real-time Alerts:
- Nhiều lần đăng nhập thất bại
- Truy cập từ IP lạ
- Thao tác bất thường (xóa nhiều records)
- Database errors
- Disk usage > 80%

---

7. Bảo mật Mạng

7.1. Firewall Rules

Inbound:
- Port 80 (HTTP): Redirect to 443
- Port 443 (HTTPS): Allow from internal network only
- Port 22 (SSH): Allow from admin IPs only
- Tất cả ports khác: DENY

Outbound:
- Allow HTTPS (443) to internet (for S3, updates)
- Allow DNS (53)
- Block tất cả trừ máy client

7.2. Network Segmentation

```
[Internet]
    |
[Firewall]
    |
[DMZ - Nginx]
    |
[Internal Network]
    |├ [App Server]
    |├ [Database Server]
    |└ [Backup Server]
```

7.3. SSL/TLS Configuration

```
# Chỉ cho phép TLS 1.2 và 1.3
ssl_protocols TLSv1.2 TLSv1.3;

# Strong ciphers only
ssl_ciphers HIGH:!aNULL:!MD5:!RC4:!DES:!3DES;
ssl_prefer_server_ciphers on;

# HSTS
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
```

---

8. Phản ứng Sự cố

8.1. Xác định Sự cố

Mức độ nghiêm trọng:

1. **Critical**: Rò rỉ dữ liệu mật, hệ thống bị xuyspecies
2. **High**: Mất quyền truy cập, downtime kéo dài
3. **Medium**: Lỗ hổng bảo mật không nghiêm trọng
4. **Low**: Vấn đề performance, logs bất thường

8.2. Quy trình Xử lý

Người phát hiện:
1. Báo cáo ngay cho SYSADMIN
2. KHÔNG phát tán thông tin
3. Ghi lại chi tiết (thời gian, hiện tượng)

SYSADMIN:
1. Đánh giá mức độ nghiêm trọng
2. Cách ly hệ thống nếu cần
3. Thu thập chứng cứ (logs, screenshots)
4. Khắc phục sự cố
5. Báo cáo lãnh đạo
6. Đánh giá và rút kinh nghiệm

8.3. Khôi phục

Mất dữ liệu:
1. Dừng hệ thống
2. Đánh giá mức độ mất mát
3. Restore từ backup gần nhất
4. Kiểm tra tính toàn vẹn dữ liệu
5. Khởi động lại hệ thống
6. Thông báo người dùng

Bị xâm nhập:
1. Cắt kết nối mạng ngay lập tức
2. Thu thập chứng cứ đầy đủ
3. Đổi tất cả mật khẩu, secrets
4. Patch lỗ hổng bảo mật
5. Kiểm tra toàn bộ hệ thống
6. Khôi phục từ backup sạch
7. Giám sát chặt chẽ 30 ngày

---

9. Tuân thủ và Kiểm tra

9.1. Kiểm tra Định kỳ

Hàng tháng:
- Review audit logs
- Kiểm tra accounts không hoạt động
- Test backup restore
- Kiểm tra permissions

Hàng quý:
- Security audit toàn diện
- Vulnerability scanning
- Penetration testing (nếu có)
- Cập nhật chính sách bảo mật

9.2. Compliance Checklist

- [ ] Tất cả users đã đọc và ký Security Policy
- [ ] Mật khẩu mặc định đã được đổi
- [ ] SSL certificates hợp lệ và chưa hết hạn
- [ ] Backup hoạt động đúng schedule
- [ ] Audit logs được review định kỳ
- [ ] Firewall rules đúng cấu hình
- [ ] Không có accounts không sử dụng
- [ ] Tất cả software đã update patches

9.3. Báo cáo

Báo cáo tháng:
- Số lượng người dùng mới
- Số lần đăng nhập thất bại

- Số sự kiện bảo mật
- Disk usage và performance

Báo cáo sự cố:
- Mô tả sự cố
- Nguyên nhân
- Tác động
- Biện pháp khắc phục
- Kiến nghị phòng ngừa

---

10. Trách nhiệm

10.1. SYSADMIN

- Quản lý hạ tầng hệ thống
- Cấu hình bảo mật
- Monitoring và phản ứng sự cố
- Backup và restore
- Cập nhật hệ thống

10.2. EIC (Editor-in-Chief)

- Quản lý quyền truy cập nội dung
- Duyệt permissions người dùng
- Đảm bảo Blind Review Policy
- Báo cáo vi phạm bảo mật

10.3. Tất cả Người dùng

- Bảo mật thông tin đăng nhập
- Không chia sẻ tài khoản
- Báo cáo hoạt động đáng ngờ
- Tuân thủ chính sách bảo mật
- Đăng xuất khi không sử dụng

---

11. Liên hệ

Báo cáo Sự cố Bảo mật

- **Email**: security@hvc.local
- **Điện thoại nội bộ**: [Số điện thoại]
- **Phòng CNTT**: [Vị trí văn phòng]

Hỗ trợ Kỹ thuật

- **Email**: it-support@hvc.local
- **Điện thoại**: [Số điện thoại]
- **Giờ làm việc**: 8:00 - 17:00 (Thứ 2 - Thứ 6)

Tài liệu phiên bản: 4.0
Ngày cập nhật: 27/12/2024
Người phê duyệt: [Lãnh đạo Phòng CNTT]
Hiệu lực: Từ ngày ký

PHỤ LỤC: Biểu mẫu

A. Biểu mẫu Cam kết Bảo mật

```
CÂM KẾẾT BẢO MẬT THÔNG TIN

Tôi, [Họ và tên], [Chức vụ], cam kết:

1. Đã đọc và hiểu rõ Chính sách Bảo mật Hệ thống
2. Tuân thủ nghiêm túc các quy định về bảo mật
3. Không chia sẻ thông tin đăng nhập với người khác
4. Báo cáo ngay các vấn đề bảo mật phát hiện
5. Chịu trách nhiệm về các hành vi vi phạm

Ngày ... tháng ... năm ...
Ký tên
[Chữ ký]
```

B. Biểu mẫu Báo cáo Sự cố

```
BÁO CÁO SỰ CỐ BẢO MẬT

1. Thời gian phát hiện: []
2. Người phát hiện: []
3. Mức độ: [ ] Critical  [ ] High  [ ] Medium  [ ] Low
4. Mô tả sự cố: []
5. Tác động: []
6. Biện pháp đã thực hiện: []
7. Tình trạng hiện tại: [ ] Đã khắc phục  [ ] Đang xử lý

Ngày báo cáo: []
Người báo cáo: []
```