이름: _____ 날짜: _____ 점수: _____

데이터 보호 및 기업 스토리지 보안 가이드

데이터 마스킹, 토큰화, 저장 시 암호화와 전송 중 암호화, 오프라인 백업

데이터 보호 학습 개요

보호됨
데이터 암호화
256비트 AES 표준

규정 준수
글로벌 표준
GDPR 및 CCPA 규정 체계

제로 트러스트
접근 정책
다중 요소 인증

환영합니다! 이 활동 자료집은 데이터 보호 표준과 통제를 안내합니다. 전체 디스크 암호화, 보안 접근 통제, 하드웨어 백업, 클라우드 보안 상태, 데이터 마스킹 기법을 살펴봅니다.

워크시트 체크포인트

- [ ] **파트 1-4: 사이버 보안과 위협 예방을 익힙니다.**
- [ ] **파트 5-7: 십자말풀이와 단어 찾기 퍼즐을 풉니다.**
- [ ] **파트 8-9: 사례 연구와 암호 도전 과제를 풉니다.**
- [ ] **파트 10: 기초 및 심화 FAQ 페이지를 살펴봅니다.**
- [ ] **파트 11: 흥미로운 실제 사실 10가지를 살펴봅니다.**
- [ ] **보너스: 빠르게 생각하기 도전**

VPN.com 사이버 보안 가이드 열기

URL: https://www.vpn.com/cybersecurity/data-protection/

나의 데이터 보호 전략 학습 로드맵

- 데이터 마스킹과 토큰화 기법을 구분하세요.
- 저장 장치는 저장 시 암호화를, 전송 구간은 TLS를 이용한 전송 중 암호화를 적용하세요.
- 랜섬웨어 대비를 위해 오프라인 상태이며 네트워크와 분리된 백업 시스템을 설계하세요.

데이터 보호 가이드 안내

객관식과 참/거짓 문제에 답하고, 단어 은행을 사용해 빈칸을 채우고, 정의를 연결하고, 십자말풀이와 단어 찾기 퍼즐을 푸세요. 데이터 보호에 대한 지식을 적용해 보세요. 마지막으로 보너스 활동인 빠르게 생각하기를 해 보세요.

데이터 보호와 기업 스토리지 보안(소개)

데이터 보호는 마스킹, 토큰화, 저장 시 데이터베이스 암호화, 안전한 전송 프로토콜을 통해 기업의 데이터 자산을 보호합니다. 네트워크가 분리된 백업을 설계하면 침입이 진행 중일 때도 핵심 데이터베이스를 복구할 수 있도록 하는 데 도움이 됩니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1. 데이터 마스킹의 주된 목적은 무엇입니까?
   - A. 개인정보를 보호하려고 민감한 식별자를 가상이지만 현실적인 문자로 대체함
   - B. 물리 서버 저장 공간을 아끼려고 대용량 데이터베이스 파일 압축하기
   - C. 보관 백업 시스템에서 오래된 고객 연락 이메일 삭제하기
   - D. 인터넷 스캔에서 데이터베이스 서버의 공용 IP 주소 숨기기

2. 데이터베이스 서버 하드 드라이브에 저장된 파일을 암호화하는 메커니즘은 무엇입니까?
   - A. 저장 상태의 전체 디스크 암호화
   - B. 전송 중인 TLS 세션 핸드셰이크 프로토콜
   - C. 동적 DNS 네임서버 전달 규칙
   - D. 하드웨어 키를 이용한 다단계 인증

3. 전송 중인 데이터를 나타내는 것은 무엇입니까?
   - A. 네트워크 라우터와 스위치를 거쳐 이동하는 데이터 패킷
   - B. 콜드 백업 드라이브에 저장된 데이터베이스 트랜잭션 로그
   - C. 격리된 클라우드 보관소에 저장된 보관 사용자 파일
   - D. 로컬 데스크톱 저장소의 정적 시스템 구성 파일

4. 랜섬웨어 대비에 정기적인 오프라인 백업이 중요한 이유는 무엇입니까?
   - A. 몸값을 내지 않고 파일을 복원할 수 있는 깨끗한 오프라인 사본을 제공함
   - B. 해커가 열린 포트 구성을 스캔하는 것을 막는다
   - C. 로컬 네트워크 전송 대역폭 속도를 높인다
   - D. 브라우저의 쿠키 동의 선택 기록을 자동화한다

5. 데이터 토큰화는 무엇을 합니까?
   - A. 민감한 카드 번호를 민감하지 않은 무작위 토큰으로 대체함
   - B. 웹 트래픽을 여러 보안 onion 노드를 거쳐 라우팅한다
   - C. 시그니처 기반 악성코드를 찾으려고 시스템 디렉터리를 검사한다
   - D. 데이터베이스 관리자의 로그인 세션 시간을 감사한다

체크포인트 2: 참/거짓 도전

6 질문 6

6. 데이터 마스킹은 운영 환경의 데이터베이스 레코드를 영구적으로 변경합니다.

○ 참 ○ 거짓

7 질문 7

7. 랜섬웨어 확산을 막으려면 오프사이트 백업은 기본 기업 네트워크와 분리해야 합니다.

○ 참 ○ 거짓

8 질문 8

8. SSL/TLS 인증서는 물리 매체에 저장된 데이터를 암호화하여 데이터베이스를 보호합니다.

○ 참 ○ 거짓

9 질문 9

9. 제로 트러스트 네트워크 접근(ZTNA)은 데이터베이스 접근을 허용하기 전에 모든 사용자의 신원을 확인합니다.

○ 참 ○ 거짓

10 질문 10

10. 볼트 기반 토큰화는 원래의 카드 값을 안전한 중앙 토큰 볼트에 저장합니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

아래 각 문장을 읽고 단어 목록에서 알맞은 용어를 골라 빈칸을 채우세요.

1. 실제 같은 대체 값으로 개인 이름을 바꾸는 것을 데이터 _____ (이)라고 합니다.
2. 물리 디스크 블록을 암호화하면 데이터베이스 자산이 _____ 상태에서도 보호됩니다.
3. TLS 프로토콜은 _____ 중인 활성 데이터 패킷을 암호화합니다.
4. 역할 기반 권한은 데이터베이스 _____ 권한을 얻을 수 있는 사용자를 제한합니다.
5. 침해 이후 깨끗한 회사 파일을 복원하려면 안전한 오프라인 _____ 이(가) 필요합니다.
6. 클라우드 설정을 감사하면 조직의 보안 _____ 을(를) 평가할 수 있습니다.

어휘 단어 목록

규정 준수 | 마스킹 | 백업 | 저장 | 전송 | 접근 | 침해 | 태세

여기에 답을 쓰세요:

1.
2.
3.
4.
5.
6.

체크포인트 4: 보안 개념 연결

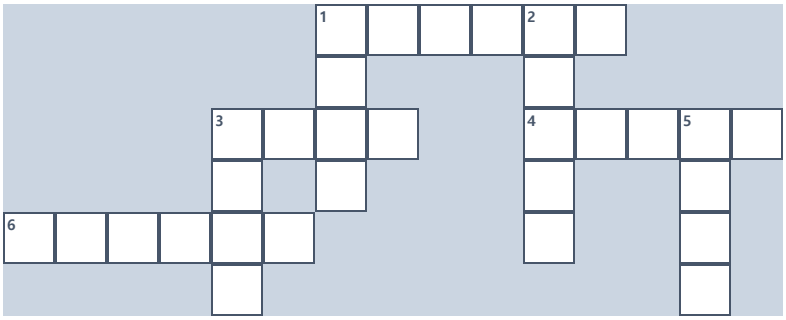
정의 연결하기

왼쪽의 각 어휘를 오른쪽의 알맞은 설명과 연결하고, 입력 칸에 해당하는 글자(A-H)를 쓰세요.

☐	**1. 암호화**	**A**	시스템 장애 시 복원할 수 있도록 데이터의 안전한 오프사이트 사본 만들기.
☐	**2. 백업**	**B**	평문을 읽을 수 없는 암호문으로 바꿔, 가로챈 데이터가 비공개로 유지되게 하는 것.
☐	**3. 최소화**	**C**	조직의 클라우드에 대한 전반적인 보안 상태와 방어 준비 태세입니다.
☐	**4. 접근**	**D**	비공개 사용자 정보를 관리하기 위한 GDPR이나 CCPA 같은 규제 기준 충족하기.
☐	**5. 보안 상태**	**E**	보호된 데이터가 승인 없이 접근되거나 공개되는 보안 사고.
☐	**6. 침해**	**F**	데이터베이스 읽기 및 쓰기 권한을 인증된 사용자 역할로 제한하는 것.
☐	**7. 규정 준수**	**G**	개인 신원을 보호하기 위해 데이터베이스 필드의 민감한 문자를 바꾸는 것.
☐	**8. 가리기**	**H**	개인 데이터 수집을 운영에 꼭 필요한 최소한으로 제한하기.

체크포인트 5: 십자말풀이

활성화된 흰색 칸에 글자를 입력해 십자말풀이를 푸세요. 숫자는 아래 열쇠에 해당합니다.



가로

1. 데이터베이스의 읽기와 쓰기 권한을 인증된 사용자 역할로 제한하는 일 (6)

3. 일에 꼭 필요한 만큼만 접근 자격을 주는 원칙 (4)

4. 민감한 값을 어떻게 가릴지 정한 기준 (5)

6. 이용자의 정보를 모으는 일 (6)

세로

1. 시스템과 자료에 들어가 쓸 수 있는 자격 (4)

2. 개인 신원을 보호하려고 데이터베이스 필드의 민감한 문자를 바꾸는 일 (5)

3. 운영에 꼭 필요한 최소한으로만 개인 데이터를 수집하도록 제한하는 일 (4)

5. 법과 업계 기준에 맞게 운영하는 일 (4)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

화면 낭독기와 키보드 사용자는 아래 입력란에 십자말풀이 정답을 직접 입력할 수 있습니다.

가로

1 가로: 데이터베이스의 읽기와 쓰기 권한을 인증된 사용자 역할로 제한하는 일 (6 글자):

3 가로: 일에 꼭 필요한 만큼만 접근 자격을 주는 원칙 (4 글자):

4 가로: 민감한 값을 어떻게 가릴지 정한 기준 (5 글자):

6 가로: 이용자의 정보를 모으는 일 (6 글자):

세로

1 세로: 시스템과 자료에 들어가 쓸 수 있는 자격 (4 글자):

2 세로: 개인 신원을 보호하려고 데이터베이스 필드의 민감한 문자를 바꾸는 일 (5 글자):

3 세로: 운영에 꼭 필요한 최소한으로만 개인 데이터를 수집하도록 제한하는 일 (4 글자):

5 세로: 법과 업계 기준에 맞게 운영하는 일 (4 글자):

체크포인트 6: 숨은 단어 찾기

아래 격자에 숨어 있는 핵심 어휘 8개를 찾으세요. 단어는 가로, 세로, 대각선으로 배치될 수 있습니다.

다 서 최 하 정 최 소 책 메 파 번 공 속 벽 트
위 킹 밀 라 요 카 다 스 최 화 개 크 칙 타 파
라 스 송 크 술 주 전 안 결 소 안 위 방 타 바
템 마 킹 다 워 터 답 용 기 킹 수 결 템 수 다
관 보 넷 파 방 개 한 데 규 격 통 집 버 격 밀
자 정 스 술 네 인 송 마 리 데 격 접 근 권 한
근 위 접 아 청 정 도 주 스 하 암 터 바 가 마
아 개 통 암 방 보 제 벽 근 킹 요 화 타 관 데
한 넷 타 술 송 수 전 벽 험 공 규 워 이 이 험
권 시 도 요 소 집 트 사 도 위 접 칙 호 템 바
소 접 근 통 제 정 책 집 카 메 준 검 아 킹 규
최 집 버 화 크 칙 카 전 타 관 한 공 사 정 응
마 가 칙 연 카 벽 나 타 접 타 안 크 준 술 카
시 험 데 하 술 스 킹 메 서 관 색 수 안 나 다
관 속 송 공 요 통 험 방 스 청 템 차 전 책 마

어휘 단어 목록

개인정보수집 최소권한 최소수집 접근통제정책 규정준수 마스킹규칙 접근권한 정보마스킹

체크포인트 6 대체 활동: 접근성을 고려한 어휘 연결

단어 찾기의 8개 어휘를 각각 알맞은 설명과 연결하고, 빈칸에 글자(A-H)를 쓰세요.

어휘 용어

- **A. 개인정보수집**
- **B. 최소권한**
- **C. 최소수집**
- **D. 접근통제정책**
- **E. 규정준수**
- **F. 마스킹규칙**
- **G. 접근권한**
- **H. 정보마스킹**

정의 및 연결 항목

1. 민감한 값을 어떻게 가릴지 정한 기준. ____
2. 개인 신원을 보호하려고 데이터베이스 필드의 민감한 문자를 바꾸는 일. ____
3. 데이터베이스의 읽기와 쓰기 권한을 인증된 사용자 역할로 제한하는 일. ____
4. 법과 업계 기준에 맞게 운영하는 일. ____
5. 시스템과 자료에 들어가 쓸 수 있는 자격. ____
6. 운영에 꼭 필요한 최소한으로만 개인 데이터를 수집하도록 제한하는 일. ____
7. 이용자의 정보를 모으는 일. ____
8. 일에 꼭 필요한 만큼만 접근 자격을 주는 원칙. ____

체크포인트 7: 뒤섞인 단어 도전

아래 글자를 맞게 배열하여 핵심 사이버 보안 개념과 용어를 알아내세요. 정답을 제공된 입력란에 쓰세요.

1. 정 개 보 수 집 인 _____
2. 최 수 집 소 _____
3. 수 규 준 정 _____
4. 한 권 접 근 _____
5. 한 최 권 소 _____
6. 정 제 접 통 책 근 _____
7. 규 칙 마 킹 스 _____
8. 킹 정 마 스 보 _____

보너스 활동: 빠르게 생각하기

각 범주마다 답을 3개씩 쓰세요. 목록을 가장 먼저 채운 사람이 이깁니다.

1	백업하는 것			
2	사이버 보안과 관련된 단어			
3	민감한 데이터를 볼 수 있는 사람			
4	데이터를 안전하게 삭제하는 방법			
5	데이터가 저장되는 장소			
6	암호화해야 하는 것			
7	병원이 보호해야 하는 데이터			
8	백업의 종류			
9	절대 공유하면 안 되는 정보			
10	이메일의 경고 신호			
11	오늘부터 시작할 수 있는 안전 습관			
12	IT 도움을 요청할 수 있는 사람			
13	해킹당할 수 있는 기기			
14	데이터를 보호하는 방법			
15	데이터를 파괴할 수 있는 것			

체크포인트 8: 사이버 보안 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사례 연구 1: 기업 데이터베이스 저장 데이터 암호화 업그레이드

👷

상황: 한 온라인 소매업체가 전체 디스크 암호화 없이 클라우드 스토리지에 거래 데이터베이스를 저장합니다. 최근 규정 준수 감사에서 이것이 심각한 CCPA 데이터 보안 위험으로 지적되었습니다. 복구 아키텍처를 설계하세요.

토론 질문: CCPA 규정 준수 위험을 분석하고, 저장 데이터 암호화 전략을 제안하세요.

사례 연구 2: 랜섬웨어 차단과 데이터 복원

👷

상황: 진행 중인 랜섬웨어 공격이 기업 로컬 네트워크의 네트워크 드라이브를 암호화하고 있습니다. 관리자는 감염을 일찍 발견했습니다. 차단 및 복구 단계를 계획하세요.

토론 질문: 즉각적인 차단 조치를 자세히 설명하고, 안전한 복원 절차를 계획하세요.

체크포인트 9: 암호 해독하기

사이버 보안 전문가는 온라인 위협 행위자로부터 네트워크 자산을 보호합니다. 아래의 자모-숫자 키를 사용해 해당하는 자모를 빈칸에 써서 메시지를 해독하세요.

자모-숫자 암호화 키

ㄱ=1 ㄲ=2 ㄴ=3 ㄷ=4 ㄸ=5 ㄹ=6 ㅁ=7 ㅂ=8 ㅃ=9 ㅅ=10
ㅆ=11 ㅇ=12 ㅈ=13 ㅉ=14 ㅊ=15 ㅋ=16 ㅌ=17 ㅍ=18 ㅎ=19 ㅏ=20
ㅐ=21 ㅑ=22 ㅒ=23 ㅓ=24 ㅔ=25 ㅕ=26 ㅖ=27 ㅗ=28 ㅘ=29 ㅙ=30
ㅚ=31 ㅛ=32 ㅜ=33 ㅝ=34 ㅞ=35 ㅟ=36 ㅠ=37 ㅡ=38 ㅢ=39 ㅣ=40

8	28	12	20	3		17	28	12	13	25	6	28

1	21	12	40	3	13	24	12	8	28		8	28	19	28

해독된 메시지:

팁: 각 숫자는 아래 키의 한글 자모 하나를 나타냅니다. 자모를 차례로 모아 글자를 만드세요(예: ㅂ+ㅗ = 보).

체크포인트 10: 기초 사이버 보안 FAQ (파트 A)

온라인 위협 대응에 관한 자주 묻는 질문과 답을 살펴보세요.

Q1: 데이터 보호란 무엇인가요?

기술적 통제를 통해 개인 및 업무 데이터를 무단 접근, 손실, 손상으로부터 보호하는 과정입니다.

Q2: 전체 디스크 암호화가 중요한 이유는 무엇인가요?

물리 드라이브에 저장된 데이터 블록을 보호하여 하드 드라이브를 물리적으로 훔쳐도 데이터를 읽지 못하게 합니다.

Q3: 저장 시 암호화와 전송 중 암호화는 어떻게 다른가요?

저장 시 암호화는 드라이브에 저장된 파일을 보호하고, 전송 중 암호화는 라우터를 통해 이동하는 활성 네트워크 패킷을 보호합니다.

Q4: 데이터 마스킹이란 무엇인가요?

신용카드 번호 같은 민감한 정보를 가상이지만 현실적인 데이터로 바꿔, 실제 기록을 노출하지 않고 테스트할 수 있게 합니다.

Q5: 오프라인 백업이 중요한 이유는 무엇인가요?

네트워크와 분리된 파일의 깨끗한 사본을 보관하여 백업이 랜섬웨어에 암호화되는 것을 막는 데 도움이 됩니다.

체크포인트 10: 기초 사이버 보안 FAQ (파트 B)

온라인 위협 대응에 관한 자주 묻는 질문과 답을 살펴보세요.

Q6: 데이터 토큰화 보관소란 무엇인가요?

무작위 토큰을 원래의 민감한 값(주 신용카드 번호 등)에 대응시켜 저장하는 안전한 격리 데이터베이스.

Q7: 제로 트러스트 데이터베이스 접근이란 무슨 뜻인가요?

네트워크 안에 있는 누구도 신뢰하지 않고, 로그인할 때마다 모든 사용자의 신원과 기기 상태를 확인한다는 뜻입니다.

Q8: TLS는 전송 중인 데이터를 어떻게 보호하나요?

TLS는 TCP 세션 페이로드를 암호화하여, 공용 네트워크의 악의적인 행위자가 전송 중인 패킷을 엿보거나 변조하지 못하게 합니다.

Q9: 데이터베이스 접근 감사란 무엇인가요?

무단 접근 패턴이나 보안 이상 징후를 탐지하기 위해 데이터베이스 쿼리와 로그인을 지속적으로 기록하는 것입니다.

Q10: 클라우드 보안 상태 감사란 무엇인가요?

열린 포트, 잘못 구성된 접근 규칙, 보안 규정 준수 격차를 찾기 위해 클라우드 구성을 분석하는 과정.

체크포인트 10: 심화 보안 FAQ (파트 C)

보안 프레임워크, 악성코드 분석, 데이터 규정 준수의 고급 기술적 측면을 탐구합니다.

Q1: 봉투 암호화는 어떻게 작동하나요?

데이터 키로 데이터를 암호화한 뒤 그 데이터 키를 마스터 키로 다시 암호화하여 키 저장과 교체를 단순화합니다.

Q2: 동형 암호화란 무엇인가요?

암호화된 데이터를 먼저 복호화하지 않고 직접 연산할 수 있게 하는 고급 암호화 방식.

Q3: 데이터베이스 열(column) 수준 암호화를 사용하는 이유는 무엇인가요?

민감한 특정 열(예: 주민등록번호 같은 SSN)을 개별적으로 암호화하여, 관리자가 테이블 전체 읽기 권한을 얻더라도 보호합니다.

Q4: 데이터 유출 방지(DLP)란 무엇인가요?

네트워크 출구 지점을 모니터링해 민감한 파일의 무단 외부 전송을 탐지하고 차단하는 소프트웨어.

Q5: 한 번 쓰고 여러 번 읽는(WORM) 백업은 랜섬웨어를 어떻게 막나요?

WORM 백업은 일정 기간 동안 파일이 삭제되거나 수정되지 않도록 막아, 랜섬웨어가 기존 백업을 암호화하는 것을 방지합니다.

체크포인트 10: 심화 보안 FAQ (파트 D)

보안 프레임워크, 악성코드 분석, 데이터 규정 준수의 고급 기술적 측면을 탐구합니다.

Q6: 키를 재사용하면 어떤 위험이 있나요?

서로 다른 데이터베이스에 같은 암호화 키를 재사용하면 키 하나가 침해될 때 모든 데이터베이스가 노출됩니다.

Q7: 데이터베이스 토큰화는 CCPA 준수를 어떻게 개선하나요?

토큰은 비운영 시스템의 레코드를 가명 처리하고 유출 피해를 제한하지만, 토큰화된 데이터도 여전히 개인정보일 수 있습니다.

Q8: 데이터 분류가 중요한 이유는 무엇인가요?

파일을 민감도 수준별로 분류하여 조직이 위험도가 높은 데이터에 가장 강력한 암호화와 접근 통제를 적용하도록 돕습니다.

Q9: 키 교체의 역할은 무엇인가요?

암호화 키를 정기적으로 갱신하면 키 하나가 결국 해독되더라도 노출되는 과거 데이터의 양이 제한됩니다.

Q10: 보안 엔클레이브는 메모리 속 데이터베이스 쿼리를 어떻게 보호하나요?

보안 엔클레이브는 CPU로 보호되는 메모리 블록 안에서 쿼리 작업을 격리해, 호스트 관리자가 RAM의 평문을 볼 수 없게 합니다.

파트 11: 실제 사이버 보안 사실 10가지와 시사점

보안 침해, 방어 메커니즘, 규정 준수 표준에 관한 실제 사실을 살펴보세요.

1. 보안 인사이트

GDPR은 2018년 5월에 시행되어 전 세계 웹사이트가 쿠키 동의와 개인정보 등록부를 관리하는 방식을 바꾸었습니다.

2. 보안 인사이트

GDPR 위반 과징금은 2천만 유로 또는 전 세계 매출의 4%에 이를 수 있어 상당한 법적 위험이 됩니다. [4]

3. 보안 인사이트

CCPA는 2020년 1월에 시행되어 미국에서 선구적인 디지털 개인정보 소비자 권리를 확립했습니다.

4. 보안 인사이트

데이터 최소화는 데이터베이스 저장 공간을 줄여 서버 운영 비용을 낮추고 유출 시 피해 규모도 줄여 줍니다.

5. 보안 인사이트

암호화 파기는 과거 백업 테이프 파일을 편집하는 대신 키를 폐기하여 백업 삭제 문제를 해결합니다.

6. 보안 인사이트

이제 전 세계 대부분의 국가가 소비자의 개인정보 권리를 보호하기 위해 개인정보 보호법을 제정했습니다.

7. 보안 인사이트

미리 체크된 상자를 사용하는 옵트인 동의 양식은 유럽 데이터 개인정보 보호 규정의 정의에 따라 명시적으로 금지됩니다.

8. 보안 인사이트

GDPR은 개인정보 침해를 인지한 때부터 가능한 경우 72시간 이내에 감독 기관에 신고하도록 요구합니다. [3]

9. 보안 인사이트

bcrypt나 Argon2 같은 느린 알고리즘으로 비밀번호를 해시하면 탈취된 해시의 오프라인 해독이 훨씬 어려워집니다. [6]

10. 보안 인사이트

저장된 데이터(data at rest)는 저장된 데이터베이스 파일을, 전송 중인 데이터(data in transit)는 네트워크 라우터를 통해 실제로 이동하는 패킷을 의미합니다.

기술 참고 자료 및 출처

이 학습 가이드와 인터랙티브 퍼즐은 전 세계 NIST, OWASP, 개인정보 보호 규정 준수 표준을 바탕으로 만들었습니다.

학술 및 업계 참고 자료

[1] NIST. (2025). SP 800-88 Rev. 2, Guidelines for Media Sanitization.
https://csrc.nist.gov/pubs/sp/800/88/r2/final

[2] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[3] Intersoft Consulting. (n.d.). Art. 33 GDPR – Notification of a personal data breach to the supervisory authority.
https://gdpr-info.eu/art-33-gdpr/

[4] Intersoft Consulting. (n.d.). Art. 83 GDPR – General conditions for imposing administrative fines.
https://gdpr-info.eu/art-83-gdpr/

[5] California Privacy Protection Agency. (n.d.). Frequently Asked Questions (FAQs).
https://cppa.ca.gov/faq.html

[6] OWASP. (n.d.). Password Storage Cheat Sheet.
https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

답안: 체크포인트 1 – 객관식

1 질문 1 정답: A

교사용 참고

데이터 마스킹의 주된 목적은 무엇입니까? → 개인정보를 보호하려고 민감한 식별자를 가상이지만 현실적인 문자로 대체함

2 질문 2 정답: A

교사용 참고

데이터베이스 서버 하드 드라이브에 저장된 파일을 암호화하는 메커니즘은 무엇입니까? → 저장 상태의 전체 디스크 암호화

3 질문 3 정답: A

교사용 참고

전송 중인 데이터를 나타내는 것은 무엇입니까? → 네트워크 라우터와 스위치를 거쳐 이동하는 데이터 패킷

4 질문 4 정답: A

교사용 참고

랜섬웨어 대비에 정기적인 오프라인 백업이 중요한 이유는 무엇입니까? → 몸값을 내지 않고 파일을 복원할 수 있는 깨끗한 오프라인 사본을 제공함

5 질문 5 정답: A

교사용 참고

데이터 토큰화는 무엇을 합니까? → 민감한 카드 번호를 민감하지 않은 무작위 토큰으로 대체함

답안: 체크포인트 2 – 참 또는 거짓

6 **질문 6** 정답: 거짓

교사용 참고

마스킹은 테스트용 복사본을 변경하거나 쿼리 시점에 값을 숨기며, 운영 기록은 그대로 유지됩니다.

7 **질문 7** 정답: 참

교사용 참고

랜섬웨어 확산을 막으려면 오프사이트 백업은 기본 기업 네트워크와 분리해야 합니다.

8 **질문 8** 정답: 거짓

교사용 참고

TLS 인증서는 전송 중인 데이터를 보호하며, 저장된 데이터에는 디스크, 파일, 데이터베이스 암호화가 필요합니다.

9 **질문 9** 정답: 참

교사용 참고

제로 트러스트 네트워크 접근(ZTNA)은 데이터베이스 접근을 허용하기 전에 모든 사용자의 신원을 확인합니다.

10 **질문 10** 정답: 참

교사용 참고

볼트 기반 토큰화는 원래 값을 안전한 토큰 볼트에 보관하며, 이 볼트가 각 토큰을 해당 데이터에 연결합니다.

어휘 정답 및 채점 기준표

교사용 채점 기준: 정확하게 연결한 항목마다 1점(총 8점), 문맥 용어마다 1점(총 6점)을 줍니다.

체크포인트 4: 답안 – 개념 연결

B 1. 암호화	A 2. 백업	H 3. 최소화	F 4. 접근
C 5. 보안 상태	E 6. 침해	D 7. 규정 준수	G 8. 가리기

체크포인트 3: 답안 – 핵심 용어

1 마스킹	2 저장	3 전송	4 접근
5 백업	6 태세		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 F – 마스킹규칙	2 H – 정보마스킹	3 D – 접근통제정책	4 E – 규정준수
5 G – 접근권한	6 C – 최소수집	7 A – 개인정보수집	8 B – 최소권한

교사를 위한 토론 참고

핵심 용어:
학생들이 암호화, 백업, 최소화를 자신의 말로 설명하고 각각 예를 들 수 있는지 확인하세요.

사례 연구:
학생들이 의견이 아니라 워크시트의 사실을 근거로 권고안을 제시하게 하세요.

출처 평가:
학생들에게 워크시트의 참고 자료로 주장을 하나 이상 확인하게 하고, 수치·가격·규정이 시간이 지나면서 바뀔 수 있는 이유를 토론하게 하세요.

퍼즐 답안과 교사용 참고

단어 찾기 정답

다	서	최	하	정	최	소	책	메	파	번	공	속	벽	트
위	킹	밀	라	요	카	다	스	최	화	개	크	칙	타	파
라	스	송	크	술	주	전	안	결	소	안	위	방	타	바
템	마	킹	다	워	터	답	용	기	킹	수	결	템	수	다
관	보	넷	파	방	개	한	데	규	격	통	집	버	격	밀
자	정	스	술	네	인	송	마	리	데	격	접	근	권	한
근	위	접	아	청	정	도	주	스	하	암	터	바	가	마
아	개	통	암	방	보	제	벽	근	킹	요	화	타	관	데
한	넷	타	술	송	수	전	벽	험	공	규	워	이	이	험
권	시	도	요	소	집	트	사	도	위	접	칙	호	템	바
소	접	근	통	제	정	책	집	카	메	준	검	아	킹	규
최	집	버	화	크	칙	카	전	타	관	한	공	사	정	응
마	가	칙	연	카	벽	나	타	접	타	안	크	준	술	카
시	험	데	하	술	스	킹	메	서	관	색	수	안	나	다
관	속	송	공	요	통	험	방	스	청	템	차	전	책	마

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

1 가로: 접근통제정책 데이터베이스의 읽기와 쓰기 권한을 인증된 사용자 역할로 제한하는 일 (6 글자)

3 가로: 최소권한 일에 꼭 필요한 만큼만 접근 자격을 주는 원칙 (4 글자)

4 가로: 마스킹규칙 민감한 값을 어떻게 가릴지 정한 기준 (5 글자)

6 가로: 개인정보수집 이용자의 정보를 모으는 일 (6 글자)

세로

1 세로: 접근권한 시스템과 자료에 들어가 쓸 수 있는 자격 (4 글자)

2 세로: 정보마스킹 개인 신원을 보호하려고 데이터베이스 필드의 민감한 문자를 바꾸는 일 (5 글자)

3 세로: 최소수집 운영에 꼭 필요한 최소한으로만 개인 데이터를 수집하도록 제한하는 일 (4 글자)

5 세로: 규정준수 법과 업계 기준에 맞게 운영하는 일 (4 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 정개보수집인 — **개인정보수집**
2. 최수집소 — **최소수집**
3. 수규준정 — **규정준수**
4. 한권접근 — **접근권한**
5. 한최권소 — **최소권한**
6. 정제접통책근 — **접근통제정책**
7. 규칙마킹스 — **마스킹규칙**
8. 킹정마스보 — **정보마스킹**

비밀 암호 도전 정답

"보안 통제로 개인정보 보호"

사례 연구 답안

A 사례 연구 1: 기업 데이터베이스 저장 데이터 암호화 업그레이드

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 시나리오 분석: 한 온라인 소매업체가 전체 디스크 암호화 없이 클라우드 저장소에 거래 데이터베이스를 보관합니다. 최근 규정 준수 감사에서 이것이 심각한 CCPA 데이터 보안 위험으로 지적되었습니다. 복구 아키텍처를 설계하세요.
- 권장 전략 및 해결책: 모든 파일 시스템에 AES-256 저장 데이터 전체 디스크 암호화를 적용하세요. 자동 키 교체 기능이 있는 중앙 집중식 키 관리 서비스(KMS)를 사용하고, 엄격한 IAM 정책으로 복호화 접근을 통제합니다.

B 사례 연구 2: 랜섬웨어 차단과 데이터 복원

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 활성 랜섬웨어 공격이 기업 로컬 네트워크의 네트워크 드라이브를 암호화하고 있습니다. 관리자는 감염을 일찍 발견했습니다. 격리 및 복구 단계를 계획하세요.
- 권장 전략 및 해결책: 침해된 네트워크 구간을 즉시 격리하세요. 영향을 받은 엔드포인트를 포맷하고 최신 오프라인 WORM(한 번 쓰고 여러 번 읽기) 백업에서 복원합니다. 시스템을 다시 연결하기 전에 백업 무결성을 확인하세요.