姓名: _____ 日期: _____ 得分: _____

数据保护与企业存储安全指南

数据脱敏、令牌化、静态加密与传输中加密、离线备份

数据保护学习概览

受保护
数据加密
256 位 AES 标准

合规的
全球标准
GDPR 与 CCPA 框架

零信任
访问策略
多重身份验证

欢迎！ 本活动手册将带你了解数据保护标准和控制措施。你将探索全盘加密、安全访问控制、硬件备份、云安全态势和数据脱敏技术。

练习单检查点

- [ ] **第 1-4 部分: 掌握网络安全和威胁防范。**
- [ ] **第 5-7 部分: 解答填字游戏和单词搜索谜题。**
- [ ] **第 8-9 部分: 解答案例研究和密码挑战。**
- [ ] **第 10 部分: 查看基础和进阶 FAQ 页面。**
- [ ] **第 11 部分: 探索 10 个有趣的现实事实。**
- [ ] **附加: 快速思考挑战。**

打开 VPN.com 网络安全指南

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

你的数据保护策略学习路线图

- 区分数据脱敏和令牌化技术。
- 对存储驱动器实施静态加密，并使用 TLS 实施传输中加密。
- 设计离线、网络隔离的备份系统以防范勒索软件。

数据保护指南说明

回答单项选择题和判断题，使用词库完成填空句，配对定义，并解答填字游戏和找词游戏。将所学知识应用于数据保护。 最后完成附加活动: 快速思考。

数据保护与企业存储安全（引言）

数据保护通过数据脱敏、令牌化、静态数据库加密和安全传输协议来保护企业数据资产。设计网络隔离的备份有助于确保在发生持续入侵时关键数据库能够恢复。

仔细阅读每个检查点，选择或写出正确的答案。

检查点 1: 单项选择挑战

1. 数据脱敏的主要目的是什么?

- A. 用虚构但逼真的字符替换敏感标识符以保护隐私
- B. 压缩大型数据库文件以节省物理服务器存储空间
- C. 从归档备份系统中删除旧的客户联系电子邮件
- D. 对互联网扫描隐藏数据库服务器的公网 IP 地址

2. 哪种机制可加密存储在数据库服务器硬盘上的文件?

- A. 静态全盘加密
- B. 传输中的 TLS 会话握手协议
- C. 动态 DNS 域名服务器转发规则
- D. 使用硬件密钥的多因素认证

3. 什么代表传输中的数据?

- A. 在网络路由器和交换机之间传输的数据包
- B. 存放在冷备份硬盘上的数据库事务日志
- C. 保存在隔离云保险库中的归档用户文件
- D. 本地桌面存储上的静态系统配置文件

4. 为什么定期离线备份对防范勒索软件至关重要?

- A. 它提供一份干净的离线副本，无需支付赎金即可恢复文件
- B. 它可以防止黑客扫描开放的端口配置
- C. 它提高本地网络传输带宽速度
- D. 它自动记录浏览器上的 Cookie 同意选择

5. 数据令牌化有什么作用?

- A. 它用非敏感的随机令牌替换敏感的卡号
- B. 它通过多个安全的洋葱节点路由网络流量
- C. 它扫描系统目录中基于特征码的恶意软件
- D. 它审计数据库管理员的登录会话时间

检查点 2: 判断正误挑战

6 问题 6

6. 数据脱敏会永久更改生产环境中的数据库记录。

○ 正确 ○ 错误

7 问题 7

7. 异地备份必须与公司主网络隔离，以防止勒索软件传播。

○ 正确 ○ 错误

8 问题 8

8. SSL/TLS 证书通过加密存储在物理介质上的静态数据来保护数据库。

○ 正确 ○ 错误

9 问题 9

9. 零信任网络访问（ZTNA）在授予数据库访问权限前会验证每个用户的身份。

○ 正确 ○ 错误

10 问题 10

10. 基于保管库的令牌化会将原始卡号存储在安全的中央令牌保管库中。

○ 正确 ○ 错误

检查点 3: 关键术语填空

阅读下面的每个句子，并从词库中选出正确的术语填空。

1. 用逼真的占位符替换个人姓名称为数据 _____ 。
2. 对物理存储块加密可保护处于 _____ 状态的数据库资产。
3. TLS 协议加密处于 _____ 中的活动数据包。
4. 基于角色的权限限制哪些用户可以获得数据库 _____ 。
5. 对泄露后会造成严重损害的 _____ 要实施严格保护。
6. 审计云配置可评估组织的安全 _____ 。

词汇词库

备份　传输　访问　静态　敏感数据　数据泄露　态势　脱敏

在此写下你的答案:

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

检查点 4: 安全概念配对

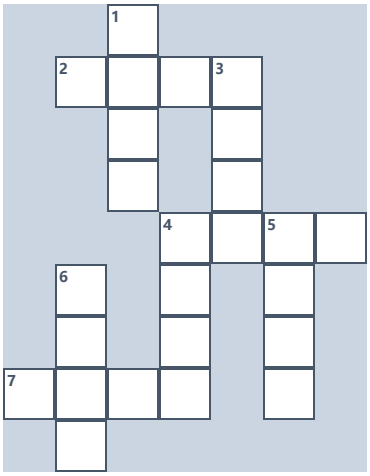
定义配对

将左侧的每个词汇与右侧正确的定义配对，在可填写的输入框中写出对应的字母（A-H）。

	1. 加密	**A**	创建安全的异地数据副本，以便在系统故障时恢复。
	2. 备份	**B**	将明文转换为不可读的密文，使被截获的数据保持私密。
	3. 最小化	**C**	组织云环境整体的安全状态和防御就绪程度。
	4. 访问	**D**	满足 GDPR 或 CCPA 等管理用户私人信息的监管标准。（G）
	5. 安全状态	**E**	受保护的数据在未经授权的情况下被访问或披露的安全事件。
	6. 数据泄露	**F**	将数据库读写权限限制在经过身份验证的用户角色。
	7. 合规	**G**	替换数据库字段中的敏感字符以保护个人身份。
	8. 屏蔽	**H**	将个人数据收集限制在运营所需的绝对最低限度。（C）

检查点 5: 填字游戏

在活动的白色方框中输入汉字，完成填字游戏。数字对应下面的提示。



横向

2. 替换数据库字段中的敏感字符以保护个人身份 (4)

4. 读取或使用保存信息的行为 (4)

7. 对存放在存储设备中的数据加密 (4)

纵向

1. 受保护数据在未经授权的情况下被访问或披露的安全事件 (4)

3. 一旦泄露会造成严重损害的资料 (4)

4. 把明文信息转换成密文的保护措施 (4)

5. 把数据库读写权限限制给经过认证的用户角色 (4)

6. 组织云环境整体的安全状况和防御准备程度 (4)

检查点 5 替代活动: 无障碍填字线索

使用屏幕阅读器和键盘的用户可以直接在下面的文本框中输入填字游戏的答案。

横向

2 横向: 替换数据库字段中的敏感字符以保护个人身份 (4 字):

4 横向: 读取或使用保存信息的行为 (4 字):

7 横向: 对存放在存储设备中的数据加密 (4 字):

纵向

1 纵向: 受保护数据在未经授权的情况下被访问或披露的安全事件 (4 字):

3 纵向: 一旦泄露会造成严重损害的资料 (4 字):

4 纵向: 把明文信息转换成密文的保护措施 (4 字):

5 纵向: 把数据库读写权限限制给经过认证的用户角色 (4 字):

6 纵向: 组织云环境整体的安全状况和防御准备程度 (4 字):

检查点 6: 隐藏单词搜索

在下方网格中找出隐藏的 8 个关键词汇。单词可以是水平、垂直或对角线方向。

全 址 隧 安 息 静 用 私 静 共 控 输 务 墙 系
攻 协 护 软 火 全 人 服 数 安 理 协 击 私 露
务 据 器 安 份 私 访 公 身 据 信 风 户 软 域
务 数 数 理 泄 络 护 址 道 问 脱 访 泄 险 传
录 感 安 设 域 静 器 名 势 认 脱 敏 软 敏 息
统 敏 火 密 管 态 访 数 保 份 备 认 统 敏 软
险 加 隧 传 公 加 用 防 据 址 数 网 数 加 击
感 防 域 感 议 密 敏 人 协 访 务 设 证 域 务
制 访 份 身 协 件 系 隐 证 证 问 件 管 传 人
控 共 护 据 输 软 险 接 理 据 录 服 输 脱 浏
问 安 全 态 势 加 泄 录 息 协 私 露 服 身 数
访 务 设 势 数 系 加 道 数 网 露 风 服 据 议
络 务 险 务 据 信 私 问 服 管 件 认 泄 用 访
理 泄 输 信 加 设 览 户 络 络 设 露 击 身 统
人 敏 件 域 密 管 人 理 码 身 制 数 息 理 势

词汇列表

静态加密 安全态势 数据加密 数据访问 敏感数据 访问控制 数据脱敏 数据泄露

检查点 6 替代活动: 无障碍词汇配对

将词语搜索中的 8 个词汇与其正确的定义配对，在空白处写出字母（A-H）。

词汇术语
A. 静态加密
B. 安全态势
C. 数据加密
D. 数据访问
E. 敏感数据
F. 访问控制
G. 数据脱敏
H. 数据泄露

定义与配对字段
1. 把数据库读写权限限制给经过认证的用户角色。
2. 受保护数据在未经授权的情况下被访问或披露的安全事件。
3. 读取或使用保存信息的行为。
4. 一旦泄露会造成严重损害的资料。
5. 替换数据库字段中的敏感字符以保护个人身份。
6. 把明文信息转换成密文的保护措施。
7. 对存放在存储设备中的数据加密。
8. 组织云环境整体的安全状况和防御准备程度。

检查点 7: 乱序单词挑战

把下面的汉字重新排列，找出关键的网络安全概念和术语。把答案写在提供的输入框中。

1. 加 静 密 态 _____

2. 数 加 密 据 _____

3. 据 敏 数 感 _____

4. 敏 脱 数 据 _____

5. 势 安 态 全 _____

6. 访 问 数 据 _____

7. 控 访 制 问 _____

8. 数 露 泄 据 _____

附加活动: 快速思考

每个类别写出 3 个答案。最先填完列表的人获胜。

1	你要备份的内容			
2	与网络安全相关的词语			
3	可以查看敏感数据的人			
4	安全删除数据的方法			
5	数据存储的地方			
6	应该加密的内容			
7	医院必须保护的数据			
8	备份的类型			
9	你绝不应分享的信息			
10	电子邮件中的警示信号			
11	你今天就可以开始的安全习惯			
12	可以向其寻求 IT 帮助的人			
13	可能被黑客入侵的设备			
14	保护数据的方法			
15	可能损毁数据的因素			

检查点 8: 网络安全案例研究

运用你所学的概念来解决下面的真实情景。

案例研究 1: 企业数据库静态加密升级



情景: 一家网络零售商将交易数据库存储在没有全盘加密的云存储上。最近一次合规审计将其标记为严重的 CCPA 数据安全风险。请设计一个恢复架构。

讨论问题: 分析 CCPA 合规风险，并提出一种静态数据加密策略。

案例研究 2: 勒索软件遏制与数据恢复



情景: 一场正在进行的勒索软件攻击正在加密企业本地网络上的网络驱动器。管理员及早发现了感染。请规划隔离和恢复步骤。

讨论问题: 详细说明立即采取的隔离措施，并规划一个安全的恢复流程。

检查点 9: 破解密码

网络安全专业人员保护网络资产免受网络威胁行为者的攻击。使用下面的汉字与数字对照表，在空白处写出对应的汉字，解密这条信息。

汉字转数字加密密钥

网=1 露=2 据=3 护=4 脱=5 人=6 制=7 势=8 敏=9 用=10

态=11 密=12 访=13 器=14 泄=15 感=16 服=17 码=18 安=19 络=20

户=21 私=22 全=23 问=24 务=25 静=26 控=27 数=28 保=29 加=30

19	23	27	7	29	4	22	6	28	3

解码后的信息:

提示: 每个数字对应下方密钥中的一个汉字。

检查点 10: 基础网络安全常见问题 (A 部分)

回顾有关缓解网络威胁的常见问题和解答。

Q1: 什么是数据保护?

这是通过技术控制措施，保护个人和企业数据免遭未经授权的访问、丢失或损坏的过程。

Q2: 全盘加密为什么重要?

它保护物理驱动器上存储的数据块，即使有人物理窃取硬盘，也无法读取其中的数据。

Q3: 静态加密与传输中加密有何区别?

静态加密保护驱动器上存储的文件，而传输中加密保护在路由器上传输的活动网络数据包。

Q4: 什么是数据脱敏?

它用虚构但逼真的数据替换敏感信息（如信用卡号），用于测试而不暴露真实记录。

Q5: 离线备份为什么重要?

它将你的文件的干净副本与网络隔离保存，有助于保护你的备份不被勒索软件加密。

检查点 10: 基础网络安全常见问题 (B 部分)

回顾有关缓解网络威胁的常见问题和解答。

Q6: 什么是数据令牌化保险库?

一个安全、隔离的数据库，将随机令牌映射到其原始敏感值（如信用卡主账号）。

Q7: 零信任数据库访问是什么意思?

这意味着在每次登录时都验证每位用户的身份和设备状态，而不是信任网络内部的任何人。

Q8: TLS 如何保护传输中的数据?

TLS 会加密 TCP 会话负载，防止公共网络上的恶意行为者嗅探或篡改传输中的数据包。

Q9: 什么是数据库访问审计?

持续记录数据库查询和登录，以发现未经授权的访问模式或安全异常。

Q10: 什么是云安全状态审计?

分析云配置以发现开放端口、配置错误的访问规则和安全合规缺口的过程。

检查点 10: 高级安全常见问题 (C 部分)

探索安全框架、恶意软件分析和数据合规的高级技术层面。

Q1: 信封加密是如何运作的?

它先用数据密钥加密数据，再用主密钥加密该数据密钥，从而简化密钥的存储和轮换。

Q2: 什么是同态加密?

一种先进的加密方法，允许直接对加密数据进行运算而无需先解密。

Q3: 为什么要使用数据库列级加密?

它单独加密特定的敏感列（如社会安全号码），即使管理员获得了对表的一般读取权限，这些数据也依然受到保护。

Q4: 什么是数据防泄漏 (DLP)?

监控网络出口点，以检测并阻止敏感文件未经授权外传的软件。

Q5: 一次写入多次读取 (WORM) 备份如何防御勒索软件?

WORM 备份可在设定时长内防止文件被删除或修改，从而阻止勒索软件加密现有备份。

检查点 10: 高级安全常见问题 (D 部分)

探索安全框架、恶意软件分析和数据合规的高级技术层面。

Q6: 密钥重复使用有什么风险?

在不同数据库中重复使用同一加密密钥，意味着一个密钥被攻破就会暴露所有数据库。

Q7: 数据库令牌化如何改善 CCPA 合规性?

令牌可对非生产系统中的记录进行假名化并限制泄露影响，但令牌化后的数据仍可能属于个人信息。

Q8: 数据分类为什么至关重要?

它按敏感程度对文件进行分类，帮助组织对高风险数据应用最强的加密和访问控制。

Q9: 密钥轮换起什么作用?

定期更新加密密钥，可以限制单个密钥最终被破解时所暴露的历史数据量。

Q10: 安全飞地如何在内存中保护数据库查询?

安全飞地将查询操作隔离在受 CPU 保护的内存块中，防止主机管理员查看 RAM 中的明文。

第 11 部分: 10 个现实中的网络安全事实与洞察

回顾有关安全漏洞、防御机制和合规标准的真实事实。

1. 安全洞察

GDPR 于 2018 年 5 月生效，改变了全球网站管理 Cookie 同意和个人数据登记的方式。

2. 安全洞察

违反 GDPR 的罚款最高可达 20 million 欧元或全球营业额的 4%，意味着巨大的法律风险。 [4]

3. 安全洞察

CCPA 于 2020 年 1 月生效，在美国开创了数字隐私方面的消费者权利。

4. 安全洞察

数据最小化可缩小数据库存储占用，降低服务器运营成本，同时减轻数据泄露的影响规模。

5. 安全洞察

加密销毁通过清除密钥而不是编辑历史备份磁带文件，解决了备份删除难题。

6. 安全洞察

全球大多数国家现已颁布个人数据保护法律，以保护消费者的隐私权。

7. 安全洞察

在欧洲数据隐私监管定义下，明确禁止使用预先勾选复选框的选择加入同意表单。

8. 安全洞察

GDPR 要求在知悉个人数据泄露后，在可行的情况下 72 小时内向监管机构报告。 [3]

9. 安全洞察

使用 bcrypt 或 Argon2 等慢速算法对密码进行哈希处理，会使离线破解被盗哈希值的难度大大增加。 [6]

10. 安全洞察

静态数据是指已保存的数据库文件，而传输中的数据是指正在网络路由器之间移动的数据包。

技术参考资料与来源

本学习指南和互动谜题根据全球 NIST、OWASP 以及数据隐私合规标准编写。

学术与行业参考资料

[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

答案: 检查点 1 – 单项选择

1 问题 1 正确答案: A

教学提示

数据脱敏的主要目的是什么？ → 用虚构但逼真的字符替换敏感标识符以保护隐私

2 问题 2 正确答案: A

教学提示

哪种机制可加密存储在数据库服务器硬盘上的文件？ → 静态全盘加密

3 问题 3 正确答案: A

教学提示

什么代表传输中的数据？ → 在网络路由器和交换机之间传输的数据包

4 问题 4 正确答案: A

教学提示

为什么定期离线备份对防范勒索软件至关重要？ → 它提供一份干净的离线副本，无需支付赎金即可恢复文件

5 问题 5 正确答案: A

教学提示

数据令牌化有什么作用？ → 它用非敏感的随机令牌替换敏感的卡号

答案: 检查点 2 – 判断题（正确或错误）

6 **问题 6** **正确答案: 错误**

教学提示

数据脱敏会修改测试副本或在查询时隐藏数值；生产记录保持不变。

7 **问题 7** **正确答案: 正确**

教学提示

异地备份必须与公司主网络隔离，以防止勒索软件传播。

8 **问题 8** **正确答案: 错误**

教学提示

TLS 证书保护传输中的数据；静态数据需要磁盘、文件或数据库加密。

9 **问题 9** **正确答案: 正确**

教学提示

零信任网络访问（ZTNA）在授予数据库访问权限前会验证每个用户的身份。

10 **问题 10** **正确答案: 正确**

教学提示

基于保管库的令牌化将原始值保存在安全的令牌保管库中，该保管库将每个令牌映射回其数据。

词汇答案与评分标准

教师评分标准: 每个正确配对得 1 分（共 8 分），每个语境术语得 1 分（共 6 分）。

检查点 4: 答案 – 概念配对

B 1. 加密	A 2. 备份	H 3. 最小化	F 4. 访问
C 5. 安全状态	E 6. 数据泄露	D 7. 合规	G 8. 屏蔽

检查点 3: 答案 – 关键术语

1 脱敏	2 静态	3 传输	4 访问
5 敏感数据	6 态势		

检查点 6 替代活动: 答案 – 词语配对

1 F – 访问控制	2 H – 数据泄露	3 D – 数据访问	4 E – 敏感数据
5 G – 数据脱敏	6 C – 数据加密	7 A – 静态加密	8 B – 安全态势

教师讨论提示

关键术语:
检查学生能否用自己的话解释加密、备份和最小化，并为每个术语举例。

案例研究:
请学生用练习单中的事实而不是个人观点来支持自己的建议。

来源评估:
请学生根据练习单的参考资料至少核实一项说法，并讨论数字、价格和规则为什么可能随时间变化。

谜题答案与教师说明

找词答案

全	址	隧	安	息	静	用	私	静	共	控	输	务	墙	系
攻	协	护	软	火	全	人	服	数	安	理	协	击	私	露
务	据	器	安	份	私	访	公	身	据	信	风	户	软	域
务	数	数	理	泄	络	护	址	道	问	脱	访	泄	险	传
录	感	安	设	域	静	器	名	势	认	脱	敏	软	敏	息
统	敏	火	密	管	态	访	数	保	份	备	认	统	敏	软
险	加	隧	传	公	加	用	防	据	址	数	网	数	加	击
感	防	域	感	议	密	敏	人	协	访	务	设	证	域	务
制	访	份	身	协	件	系	隐	证	证	问	件	管	传	人
控	共	护	据	输	软	险	接	理	据	录	服	输	脱	浏
问	安	全	态	势	加	泄	录	息	协	私	露	服	身	数
访	务	设	势	数	系	加	道	数	网	露	风	服	据	议
络	务	险	务	据	信	私	问	服	管	件	认	泄	用	访
理	泄	输	信	加	设	览	户	络	络	设	露	击	身	统
人	敏	件	域	密	管	人	理	码	身	制	数	息	理	势

填字游戏答案



填字游戏答案教师指南

横向

2 横向: 数据脱敏 替换数据库字段中的敏感字符以保护个人身份 (4 字)

4 横向: 数据访问 读取或使用保存信息的行为 (4 字)

7 横向: 静态加密 对存放在存储设备中的数据加密 (4 字)

纵向

1 纵向: 数据泄露 受保护数据在未经授权的情况下被访问或披露的安全事件 (4 字)

3 纵向: 敏感数据 一旦泄露会造成严重损害的资料 (4 字)

4 纵向: 数据加密 把明文信息转换成密文的保护措施 (4 字)

5 纵向: 访问控制 把数据库读写权限限制给经过认证的用户角色 (4 字)

6 纵向: 安全态势 组织云环境整体的安全状况和防御准备程度 (4 字)

乱序单词与密码答案

词汇还原练习和秘密密码挑战的评分答案。

汉字重组答案

1. 加静密态 → **静态加密**
2. 数加密据 → **数据加密**
3. 据敏数感 → **敏感数据**
4. 敏脱数据 → **数据脱敏**
5. 势安态全 → **安全态势**
6. 访问数据 → **数据访问**
7. 控访制问 → **访问控制**
8. 数露泄据 → **数据泄露**

秘密密码挑战答案

“安全控制保护私人数据”

案例研究答案

A 案例研究 1: 企业数据库静态加密升级

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一家在线零售商把交易数据库存放在没有全盘加密的云存储上。最近一次合规审计将此标记为严重的 CCPA 数据安全风险。请设计一个恢复架构。
- 推荐策略与解决方案: 在所有文件系统上实施 AES-256 静态全盘加密。使用具有自动轮换功能的集中式密钥管理服务（KMS），并执行严格的 IAM 策略来控制解密访问。

B 案例研究 2: 勒索软件遏制与数据恢复

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一次活跃的勒索软件攻击正在加密企业本地网络上的网络驱动器。管理员及早发现了感染。请规划遏制和恢复步骤。
- 推荐策略与解决方案: 立即隔离被入侵的网段。格式化受影响的终端，并从最新的离线一次写入多次读取（WORM）备份中恢复。在重新连接系统之前验证备份的完整性。