


Prep4Away

Prep4Away

> Contact Us  Login / Register

HOME

ALL VENDORS

★ GUARANTEE

? FAQ

TESTIMONIALS

CART (1)



Try **PDF Demo** before you buy

We're not the only ones **happy** about Prep4away Practice Material ...

56295+ customers in 100+ countries use Prep4away Test Engine. Meet our customers.

 iMessenger

 VOREED

 GetCustom

 JET ORANGE

 iCompany

 Paradoxx



<http://www.prep4away.com/>

Latest Certification Exam Questions & Braindumps - Prep4Away

Exam : **EX0-105J**

Title : Information Security
Foundation based on
ISO/IEC 27002

Vendor : EXIN

Version : DEMO

QUESTION NO: 1

あなたは宅配業者SpeeDeliveryのオーナーです。配送を待つ間に他の作業を実行できる少数の人を雇用します。しかし、あなたはこの時間を使って自分のプライベートメールを送信し、インターネットをサーフィンすることに気づきます。法的には、どのようにしてインターネットと電子メール機能の使用を最善に規制することができますか

A.

特定のWebサイトにアクセスできなくなり、添付ファイルを電子メールでフィルタリングするアプリケーションをインストールします。

B.

特定のWebサイトにアクセスできなくなり、添付ファイルを電子メールでフィルタリングするアプリケーションをインストールします。

C. プライバシー規定を実施します。

D. ウイルススキャナのインストールします。

Answer: B

QUESTION NO: 2

サーバールームにエアコンが設置されているのはなぜですか。

A.

サーバ室では、空気を冷却しなければならず、装置によって生成される熱を抽出しなければなりません。室内の空気も除湿され、濾過されます。

B. 企業がオフィスをやりたい場合、サーバールームが最適です。

このように、このような大規模な機器ではオフィススペースを犠牲にする必要はありません。

C.

メンテナンススタッフがあまりにも暖かいサーバールームで作業しなければならないのは楽しいことではありません。

D. バックアップテープは高温に耐えられない薄いプラスチックから作られています。

したがって、サーバールームで暑すぎると破損する可能性があります。

Answer: A

QUESTION NO: 3

文書の分類を変更する権限があるのは誰ですか。

A. 文書の著者

B. 文書の管理者

C. 文書の所有者

D. 文書所有者のマネージャー

Answer: C

QUESTION NO: 4

Midwest Insuranceは情報を保護するために多くの手段を講じています。

それは情報セキュリティ管理システムを使用し、アプリケーションのデータの入出力が検証され、機密文書が暗号化形式で送信され、スタッフがトークンを使用して情報システムにアクセスします。どれが技術的対策ではありませんか。

A. 情報セキュリティマネジメントシステム

- B. 情報システムへのアクセスを得るためのトークンの使用
- C. アプリケーションでの入出力データの検証
- D. 情報の暗号化

Answer: A

QUESTION NO: 5

物理的なセキュリティ手段の例は何ですか。

- A. スタッフがクリアデスクポリシーに従うことを要求し、作業日の終わりに機密情報が机の上に目に見えないようにする行動規範
- B. 視覚的に身に着けなければならないパスを持つアクセス制御ポリシー
- C. 機密情報の暗号化
- D. アルゴンなどの不活性ガスを含む特殊消火器

Answer: D

QUESTION NO: 6

企業情報へのアクセスを制御するためには、どのような物理的なセキュリティ対策が必要ですか。

- A. 空調
- B. ユーザー名とパスワード
- C. 右側のロック、フレーム、およびヒンジ付き耐ブレイクガラスとドアの使用
- D. USBスティックの使用を禁止する

Answer: C

QUESTION NO: 7

なぜ組織は情報セキュリティポリシーを持っていますか。

- A. 組織内のPlan-Do-Check-Actサイクルの運用を実証するために
- B. スタッフが法律を守らないようにするために
- C. 情報セキュリティが組織内でどのように設定されるかの方向性を示すために
- D. 誰もがバックアップ手順を実行する担当者を知っていることを確実にするために

Answer: C

QUESTION NO: 8

あなたは中堅企業のIT部門で働いています。機密情報が何度か間違った手に入りました。これは会社のイメージを傷つけています。あなたは会社のラップトップのための組織のセキュリティ対策を提案するよう求められました。取るべき最初のステップは何ですか。

- A. モバイルメディア (PDA、ラップトップ、スマートフォン、USBスティック) に関するポリシーを策定します。
- B. セキュリティ担当者を任命します。
- C. ラップトップとUSBスティックのハードドライブを暗号化します。
- D. アクセス制御ポリシーを設定します。

Answer: A

QUESTION NO: 9

あなたは大規模な組織で働きます。自分の立場でアクセスできない機密情報にアクセスすることができることになると気づきます。このセキュリティインシデントをヘルプデスクに報告します。

インシデントサイクルが開始されます。セキュリティインシデントサイクルの段階は何ですか。

- A. 脅威、被害、インシデント、回復
- B. 脅威、被害、回復、インシデント
- C. 脅威、インシデント、損傷、回復
- D. 脅威、回復、インシデント、被害

Answer: C

QUESTION NO: 10

あなたの組織には25台のワークステーション用のスペースを持つオフィスがあります。これらのワークステーションはすべて装備され、使用されています。再編成のために10台の追加ワークステーションが追加され、そのうち5台は1日24時間コールセンターに使用されます。5台のワークステーションが常に利用可能でなければなりません。これを確実にするためには、どのような物理的なセキュリティ対策が必要ですか。

A.

余分なオフィスを用意し、10台のワークステーションをセットアップします。したがって、機能していない機器の交換に使用できる余分な機器が必要になります。

B.

余分なオフィスを用意し、10台のワークステーションをセットアップします。夜間や夜間に警備員がいることを確認し、スタッフが安全かつ確実に勤務できるようにします。

C.

余分なオフィスを確保し、10台すべての新しいワークステーションを緊急電源装置およびUPS (無停電電源装置) に接続します。アクセスコントロールシステムを新しいスタッフの勤務時間に合わせて調整します。

建物のセキュリティ担当者に夜間や夜間にも作業が行われることを伝えます。

D.

余分なオフィスを用意し、5つの最も重要なワークステーション用のUPS (無停電電源装置) を用意します。

Answer: C

QUESTION NO: 11

次の対策のうち予防措置はどれですか。

A. システムの変更を認識できるようにするロギングシステムをインストールします

B.

ハッカーが会社のシステムにアクセスした後、すべてのインターネットトラフィックをシャットダウンします。

C. 機密情報を金庫に置きます。

D.

脅威に対処するコストが危険な情報の価値よりも高いため、リスクを許容可能と分類します。

Answer: C

QUESTION NO: 12

リスク分析にはどのようなものが使用されていますか。

- A. リスク分析は組織の情報価値を金銭的に表すために使用されます。
- B. リスク分析は管理者に責任を明確にするために使用されます。
- C. リスク分析はリスクを許容レベルまで低減するためのセキュリティ対策と併用されます。
- D. リスク分析はセキュリティ対策が費用対効果の高いタイムリーな方法で確実に展開されるようにするために使用されます。

Answer: D