ICT Berufsbildung
Formation professionnelle
Formazione professionale

Directives d'évaluation des prestations

Numéro de module	**231**
Titre du module	**Appliquer la protection et la sécurité des données**
Titre	**DEP Module 231 Eléments - Brochure sécurité, examen écrit individuel**

Aperçu	DEP en deux parties avec la réalisation d'une brochure de sécurité et un examen écrit individuel.

Nombre d'éléments	2
Numéro de l'élément	1

Description	Sur la base d'un scénario, identifier des risques, proposer des mesures de sécurités propres à l'environnement d'utilisation des ressources informatiques conformément aux lois en vigueur. Réaliser une brochure sécurité à l'attention des employé- e- s.

Objectifs opérationnels

2	Connaître des techniques de protection d'accès, des gestionnaires de mots de passe et les principes de la gestion des mots de passe. Connaître la différence entre authentification et autorisation.
3	Connaître des procédures d'enregistrement des données et de conservation délibérément redondante des données (p. ex. local, serveur, cloud). Connaître divers dangers auxquels sont exposées les données (p. ex. vol, rançongiciel, violation de l'intégrité).
5	Connaître la problématique relative à l'effacement des données dans toutes les archives et sauvegardes. Connaître les principales conditions juridiques et particularités des sites Web (p. ex. mentions légales, clause de non-responsabilité, conditions générales).

Forme de l'épreuve	Brochure de sécurité

Pondération	50%
Durée indicative (recommandation)	Temps nécessaire à l'élaboration (travail personnel)

Critères d'évaluation.	70% Pertinence technique 30% Présentation, forme et ergonomie de la brochure

info@ict-berufsbildung.ch
www.ict-berufsbildung.ch

Moyens d'aide	Support de cours
Relation à la pratique	Permettre aux utilisateur- trice- s de moyens informatiques d'adopter un comportement adéquat et d'appliquer des règles de bonnes pratiques en matière de sécurité informatique.

Nombre d'éléments	2
Numéro de l'élément	2

Description	Sur la base d'un scénario, identifier des risques, proposer des mesures de sécurités propres à l'environnement d'utilisation des ressources informatiques conformément aux lois en vigueur.

Objectifs opérationnels

1	Connaître diverses catégories permettant de classifier la sensibilité des données et leurs critères. Connaître la différence entre protection des données et sécurité des données. Connaître divers espaces juridiques (Suisse, UE). Connaître les œuvres juridiques spécifiques à leur espace (p. ex. LPD, RGPD de l'UE).
2	Connaître des techniques de protection d'accès, des gestionnaires de mots de passe et les principes de la gestion des mots de passe. Connaître la différence entre authentification et autorisation.
3	Connaître des procédures d'enregistrement des données et de conservation délibérément redondante des données (p. ex. local, serveur, cloud). Connaître divers dangers auxquels sont exposées les données (p. ex. vol, rançongiciel, violation de l'intégrité).
4	Connaître les différences fondamentales entre les lois sur la protection des données des divers espaces juridiques.
5	Connaître la problématique relative à l'effacement des données dans toutes les archives et sauvegardes. Connaître les principales conditions juridiques et particularités des sites Web (p. ex. mentions légales, clause de non-responsabilité, conditions générales).

Forme de l'épreuve	Examen écrit individuel

Pondération en	50%
Durée indicative (recommandation)	60 minutes

Critères d'évaluation.	100% des réponses correctes100% des analyses de risques correctes.

Moyens d'aide	Aucun

Relation à la pratique	Comprendre, identifier et adopter un comportement approprié face aux défis de la protection et de la sécurités des données. Analyser des situations et proposer des mesures de sécurité et justifier les solutions déployée.