CONCOURS INTERNE ET DE 3ème VOIE DE TECHNICIEN TERRITORIAL

SESSION 2020

REPORTÉE À 2021

ÉPREUVE DE RAPPORT TECHNIQUE

ÉPREUVE D'ADMISSIBILITÉ :

Élaboration d'un rapport technique rédigé à l'aide des éléments contenus dans un dossier portant sur la spécialité au titre de laquelle le candidat concourt.

Durée : 3 heures
Coefficient : 1

SPÉCIALITÉ : INGÉNIERIE, INFORMATIQUE ET SYSTÈMES D'INFORMATION

INDICATIONS DE CORRECTION

Sujet :

Vous êtes technicien territorial principal de 2ème classe au sein de la direction des systèmes d'information (D.S.I.) de la commune de Techniville (80 000 habitants).

La Directrice générale des services (D.G.S.), à la demande du Maire de la commune, envisage la mise en place du télétravail pour une partie du personnel communal. Dans ce cadre, elle interroge la direction des systèmes d'information sur les mesures à mettre en place pour offrir aux futurs télétravailleurs les moyens informatiques nécessaires tout en assurant la sécurité du système d'information de la collectivité.

Dans un premier temps, votre supérieur hiérarchique, le directeur des systèmes d'information, vous demande de rédiger à son attention, exclusivement à l'aide des documents joints, un rapport technique sur le télétravail et la sécurité informatique.

1) Présentation du sujet

Le sujet proposé aborde un thème à caractère opérationnel (la mise en place du télétravail) sous l'angle des contraintes et obligations qu'il implique en termes d'organisation et de sécurisation du système d'information. Il permet donc de replacer le candidat dans le contexte général du fonctionnement d'une collectivité tout en faisant appel à ses capacités d'analyse et à ses connaissances techniques personnelles.

Le candidat aura à restituer les contraintes techniques qu'implique le « nomadisme numérique » (sécurisation des matériels, des connexions, du réseau interne, des données…) ainsi que les mutations que ce mode de fonctionnement impose (BYOD, SaaS, Cloud…).

Le candidat devra faire appel à ses connaissances personnelles en matière de sécurité informatique, de réglementation (RGPD), d'architecture d'un système d'information (infrastructure, matériels, logiciels…) mais aussi en matière de gestion de projet (accompagnement / formation / sensibilisation des utilisateurs, collaboration transversale avec d'autres services de la collectivité).

2) Analyse de la mise en situation et du dossier

Les documents figurant dans le dossier apportent des éléments d'information permettant d'appréhender les différents aspects de la problématique posée, mais également d'entrevoir les propositions opérationnelles à formuler pour répondre à la commande.

Les informations fournies par le dossier sont à la fois techniques et organisationnelles, et composées d'éléments de diagnostic, de retours d'expérience, et de préconisations.

Certains aspects non présents dans le dossier pourront être abordés par le candidat (ex : nécessité d'évolution du SIRH liée à la mise en place du télétravail…).

Liste des documents :

Document 1 : « 8 bonnes pratiques pour bien installer le télétravail en entreprise » - Naéva Measso - *hubone.fr* – 24 octobre 2016 - 2 pages.

- Document « introductif » sur les outils informatiques et les moyens disponibles pour une mise en place efficace du télétravail.
- En termes de sécurité et de disponibilité du SI : notions de VPN et de SaaS, qui seront développées dans d'autres documents.

Document 2 : « Le travail nomade exige de repenser en profondeur la sécurisation des données des entreprises » - Alexandre Grellier - *lesechos.fr* - 9 janvier 2019 - 2 pages.

- Nomadisme : enjeu de sécurité des données
- Obligation de sécurité liée au RGPD
- Nécessité d'une collaboration étroite entre DSI et DRH tout au long du processus de mise en place du télétravail
- Mise en place de solutions de cryptage des données, virtualisation des postes de travail, stockage des données en mode cloud
- Veille à mettre en place sur les apports de l'intelligence artificielle en matière de monitoring

Document 3 : « Ce que le Cloud apporte aux travailleurs nomades » - Colin Steele - *lemagit.fr* - avril 2019 - 2 pages.

- Les solutions EFSS (Enterprise File Sync-and-Share) apportent souplesse et disponibilité des données aux utilisateurs, tout en offrant davantage de sécurité que les solutions de cloud privé qu'ils seraient tentés d'utiliser dans le cadre du télétravail
- Intérêt de la virtualisation des postes de travail (VDI, Virtual Desktop Infrastructure) en mode cloud (Desktop as a Service) et du SaaS pour favoriser l'accessibilité des données et des applications

Document 4 : « Guide ANSSI - Recommandations sur le nomadisme numérique » (Extrait) - *ANSSI* - octobre 2018 - 6 pages.

- Le risque majeur du télétravail réside dans le degré d'exposition des données auxquelles l'utilisateur a accès depuis son domicile, ou l'espace de coworking par exemple
- Redéfinition des objectifs de sécurité pour tendre vers un niveau de sécurité nomade le plus proche possible de celui du réseau interne
- Mise en place de mécanismes de protection à chaque élément du SI : aux niveaux utilisateurs, équipements, connexions…
- Mise en place d'une gestion fine et documentée des utilisateurs nomades, qui doivent être identifiés authentifiés au niveau de chaque équipement utilisé
- Nécessité de formation et de sensibilisation des utilisateurs à la sécurité numérique
- Proscrire le BYOD, restreindre la possibilité d'installation d'applications via une solution de Mobile Device Management

Document 5 : « Télétravail et RGPD : comment éviter la faille de sécurité ? » - Me Pierre-Randolph Dufau - *itforbusiness.fr* - février 2019 - 1 page.

- Nécessité de prévoir des mesures spécifiques en matière de sécurité des données, liées au respect du RGPD
- Sécurisation des accès, cryptage des données
- Sensibilisation des utilisateurs, adaptation de la charte informatique pour prendre en compte les risques liés au télétravail

Document 6 : « Le télétravail dans les trois versants de la fonction publique - Bilan du déploiement » (Extrait) - *Ministère de l'action et des comptes publics* - décembre 2018 - 4 pages.

- Retour d'expérience sur la mise en œuvre opérationnelle du télétravail dans des structures publiques : notions de coûts des équipements nécessaires, problématique de qualité de la connexion internet personnelle du télétravailleur
- Veiller à la conformité électrique du lieu de télétravail pour prévenir les dommages aux matériels utilisés
- Associer étroitement la DSI pour formaliser les prérequis indispensables de l'environnement numérique de travail de l'agent télétravailleur
- Prendre les mesures nécessaires pour favoriser l'accès à distance aux applications métier pour éviter des solutions de contournement non sécurisées (clés USB, transmission d'informations par mail, utilisation de matériels personnels)
- Information complète de l'agent sur la sécurité des données

Document 7 : « BYOD : quelles sont les bonnes pratiques ? » - *cnil.fr* - février 2019 - 2 pages.

- Le BYOD ne doit être qu'une pratique subsidiaire
- Si l'utilisation de terminaux personnels s'avère indispensable, mettre en œuvre des mesures de sécurité telles que le chiffrement des flux (VPN notamment), une authentification forte, l'effacement à distance des données professionnelles en cas de perte ou de vol…
- Respect des règles liées à la vie privée de l'agent

Document 8 : « 3 risques de sécurité IT à gérer pour protéger les ressources des télétravailleurs sans impacter leur productivité » - William Culbert - *beyondtrust.com* - avril 2019 - 2 pages.

- Problème de sécurité lié au mode de connexion personnel (routeur) qui limite l'accès à distance au terminal utilisé
- Equilibre à trouver entre coûts et risques dans le choix du matériel utilisé : personnel ou fourni par l'employeur
- Adopter une solution cloud permettant de rajouter des couches de sécurité lors de la connexion à distance
- Veille indispensable sur l'évolution des outils de cybersécurité, connaissance du rôle et des missions de chaque télétravailleur pour adapter les mesures de sécurité

Document 9 : « Zero Trust, la clé d'une transformation numérique réussie » Xavier Daspre - *journaldunet.com* - mai 2018 - 2 pages.

- La mise en place du télétravail participe à l'élargissement du périmètre du système d'information et donc une surface d'exposition accrue aux risques
- Les typologies de terminaux connectés au réseau se diversifient, les types d'attaques se multiplient et se renouvellent, les utilisateurs finaux sont bien souvent insuffisamment formés à la cybersécurité
- La mise en place d'un périmètre cloud en tant que réseau principal permet de tout considérer comme étant extérieur au réseau et de s'engager dans une démarche Zero Trust pour accroître la sécurité

Document 10 : « Télétravail et travail mobile : comment réduire le risque de fuite de données ? » - Jan Van Vliet - *L'Usine nouvelle* - novembre 2018 - 2 pages.

- L'évolution des pratiques en matière de télétravail et de travail mobile oblige à repenser la politique de sécurité du SI sans impacter la productivité des employés.
- Mise en place d'une vraie politique de responsabilisation des employés par rapport à la fuite de données
- Enjeu majeur de chiffrement des données contenues dans les appareils ou échangés par messagerie
- Le déploiement d'une solution de DLP (Data Loss Prevention) permet de limiter les risques liés à la fuite de données sensibles

3) Proposition de plan détaillé

Avertissement : *il s'agit d'une proposition de plan, et non d'un plan type.*

En-tête

Comme indiqué dans la note de cadrage de l'épreuve, il est attendu une présentation du rapport sous la forme suivante :

Collectivité de Techniville

RAPPORT TECHNIQUE
à l'attention de M. le Directeur des Systèmes d'Information

Objet : Les enjeux de sécurité informatique liés à la mise en place du télétravail

Introduction

*Rappel du cadrage : Le rapport avec propositions doit comporter **une unique introduction** d'une vingtaine de lignes rappelant le contexte et comprenant impérativement **l'annonce de chacune des deux parties** (partie informative / partie propositions). Les candidats doivent veiller à ce que l'annonce du plan aille au-delà d'une simple annonce de la structure de la copie et porte sur le contenu précis de chacune des parties.*

Éléments pouvant être abordés en introduction :

- Assouplissement des conditions du recours au télétravail
- Volonté politique pour sa mise en place au sein de la commune de Techniville
- La mise en place du télétravail revêt des enjeux de sécurité à plusieurs niveaux : au niveau du système d'information, au niveau des agents télétravailleurs, au niveau des données
- Des propositions opérationnelles doivent être faites en amont et une collaboration étroite avec la Direction Générale et la DRH doit être mise en place

Plan détaillé

I. La mise en place du télétravail au sein de la commune de Techniville : des enjeux de sécurité à différents niveaux

A. Télétravail et nomadisme numérique : une indispensable adaptation du système d'information

- Conséquence de ces nouvelles pratiques professionnelles : l'élargissement du périmètre du système d'information, il ne se limite plus au seul réseau interne (doc 9)
- Enjeu principal : renforcer la sécurité tout en n'altérant pas la productivité des agents (docs 1, 8)
- Objectif : tendre vers une sécurité du système d'information « nomade » équivalente au SI actuel (doc 4)
- Nécessité de déployer les solutions indispensables à la sécurité avant la mise en place du télétravail afin d'éviter des solutions de contournement génératrices de risques accrus (doc 6)

B. Des enjeux de sécurité aux niveaux utilisateurs et données

- Une méconnaissance des risques de la part des utilisateurs (docs 9, 10)

- La mise en place du télétravail implique une exposition accrue des données aux risques (doc 4)
- Le RGPD vient renforcer les obligations de sécurisation des accès aux données (docs 2, 5)
- Nécessité d'établir des prérequis techniques concernant l'environnement numérique de travail des agents concernés (doc 6)
- Le choix entre mise à disposition des télétravailleurs du matériel informatique ou utilisation de leur matériel personnel : un nécessaire arbitrage entre coût et risques (docs 7, 8)

II. Télétravail et sécurisation du SI de Techniville : des évolutions techniques et organisationnelles

A. Des solutions techniques pour sécuriser le SI

- Mise en place de connexions sécurisées de type VPN, de solutions cloud pour faciliter et sécuriser l'accès aux données, migration des applications en mode SaaS, (docs 1, 2, 8)
- Mettre en œuvre la virtualisation des postes de travail, le chiffrement des données (doc 2, 3, 10)
- renforcer la gestion et l'authentification des utilisateurs, la sécurisation des équipements et de leurs contenus par des solutions de type MDM et DLP (docs 4, 7, 10)
- limiter l'utilisation de matériels personnels dans le cadre professionnel (docs 4, 7)
- envisager une démarche de type « zero trust » pour anticiper l'ouverture croissante du SI vers l'extérieur (doc 9)

B. Le développement du télétravail comme moteur d'évolutions organisationnelles

- Les changements d'organisation du travail doivent s'accompagner de changements des comportements : sensibilisation des utilisateurs aux risques, formation aux bonnes pratiques liées à la sécurité informatiques et adaptation de la charte informatique (docs 5, 6)
- Association étroite - tout au long de la mise en place du projet - entre les directions concernées (direction générale, ressources humaines), le délégué à la protection des données et la DSI (doc 6)
- Renforcer la veille technologique et le monitoring pour gagner en réactivité en cas de menaces avérées et adapter le SI aux nouvelles techniques et bonnes pratiques en matière de sécurité (docs 2, 8)

Conclusion

Rappel du cadrage : la conclusion est facultative. Elle peut toutefois utilement souligner l'essentiel, sans jamais valoriser les informations oubliées dans le développement.