E5 – IR

C02 : ORGANISER UNE INTERVENTION

Les différents interlocuteurs et ressources sont identifiés

- ☐Le rôle des différents interlocuteurs est connu.
- ☐La liste des équipements/logiciels à prévoir est exhaustive.
- ☐Les impacts des exigences sur les autres systèmes sont identifiés.
- ☐Les tâches professionnelles à exécuter sont identifiées.

Le cahier des charges préliminaire est complété et les ressources permettant de répondre au cahier des charges sont décrites

- ☐Les fonctions principales du cahier des charges peuvent être complétées par des fiches d'intervention.
- ☐Chaque fiche d'intervention contient la liste des étapes de l'intervention et les ressources nécessaires.
- ☐Chaque fiche d'intervention est détaillée avec un plan d'adressage et des diagrammes (réseaux, SYSML …)
- ☐La continuité de service est prise en compte.

Le planning prévisionnel est interprété

- ☐Un outil de répartition des tâches est utilisé (Gantt, Kanban …)
- ☐Les intervenants et leurs rôles sont identifiés.
- ☐Les dépendances entre les tâches sont identifiées.
- ☐Le chemin critique est identifié et quantifié.

Face à un ensemble de faits, des actions appropriées à poser sont décidées
De façon à poser des actions au moment opportun dans un contexte déterminé, la prise en charge est adaptée selon les responsabilités
Le travail est préparé de façon à satisfaire les exigences de qualité, d'efficacité et d'échéancier

C06 : VALIDER UN SYSTÈME INFORMATIQUE

Les environnements sont choisis et justifiés, les données de l'entreprise sont identifiées

- ☐Le périmètre d'intervention est identifié en utilisant un diagramme réseau et/ou SYSML.
- ☐Les interactions et les caractéristiques des communications avec les autres systèmes sont identifiées.
- ☐Les outils de diagnostic sont identifiés.
- ☐Les paramétrages existants sont identifiés.

Les procédures de test sont établies

- ☐Un document listant les exigences et les tests associés peut être rédigé sous forme d'un cahier de recette.
- ☐Le document est organisé en suivant une démarche logique.
- ☐Le document est exhaustif, chaque test est associé à une exigence.
- ☐Une automatisation des tests est proposée.

Les tests (unitaires, d'intégration et autres) sont appliqués

- ☐Les tests sont réalisés conformément aux procédures avec les appareils ou logiciels adéquats.
- ☐Les outils de diagnostic sont correctement utilisés.
- ☐Le résultat de chaque test et son incertitude, est correctement appréhendé.
- ☐Le cahier de recette peut être complété avec les résultats obtenus.

Les résultats de tests sont synthétisés pour évaluer la conformité globale

- ☐Les résultats des tests et leurs incertitudes sont correctement interprétés.
- ☐Les anomalies sont identifiées, le PV d'anomalie est rédigé.
- ☐Un diagnostic des anomalies est posé, la documentation relative à l'installation est éventuellement mise à jour.
- ☐Un bilan au regard des exigences est établi.

Le document de recette est validé par le client et la recette est réalisée avec le client

- ☐Les étapes de recette sont énoncées clairement au client.
- ☐Le vocabulaire utilisé est adapté au client. Le discours est clair et structuré.
- ☐Le cahier de recette (PV de livraison) est rempli et validé avec le client.
- ☐Le client pourra être conseillé sur les futures actions de maintenance du système et les points de vigilance de la cybersécurité.

Le travail est préparé de façon à satisfaire les exigences de qualité, d'efficacité et d'échéancier
Le calme est conservé de façon constante dans des situations particulières, tout en persévérant dans la tâche jusqu'à l'atteinte du résultat sans se décourager
Face à un ensemble de faits, des actions appropriées à poser sont décidées

C09 : INSTALLER UN RÉSEAU INFORMATIQUE

Les équipements nécessaires à la réponse au CDC (fourni par le client) sont identifiés

- ☐Les différents éléments matériels du réseau sont identifiés
- ☐Le rôle des différents éléments est explicité.
- ☐Un schéma réseau les présente
- ☐Les protocoles réseaux et de communication répondant au CDC sont choisis et explicités.

Une procédure de configuration ou d'installation est déterminée ainsi que les points critiques, les procédures étant soumises à validation si nécessaire

- ☐Les étapes de configuration ou d'installation sont détaillées.
- ☐Les paramètres de configuration choisis sont cohérents.
- ☐Un plan d'adressage cohérent est rédigé ou complété.
- ☐Les enjeux de la cybersécurité sont pris en compte.

La ou les procédures choisies sont suivies

- ☐La procédure est exécutée, un compte-rendu de l'avancement est effectué.
- ☐Les fichiers de configuration sont sauvegardés.
- ☐Si la procédure contient des oublis, ils sont identifiés.
- ☐Si la procédure échoue, un correctif est proposé.

Les activités sont menées en respectant les règles de sécurité

- ☐Les niveaux d'habilitation (cybersécurité, électrique, secret …) sont identifiés et respectés.
- ☐Les politiques de sécurité (des personnes, des données, des réseaux) sont suivies.
- ☐Les mises à jour de sécurité, les scripts de mise à jour automatique sont déployés.
- ☐Les documents sont protégés, les accès systèmes sont surveillés et protégés.

Un compte-rendu du fonctionnement de l'installation est fourni (anomalies, difficultés et retours clients etc.)

- ☐Un compte-rendu est rédigé, avec la procédure de configuration complétée.
- ☐Le compte rendu des configurations recense les sauvegardes des fichiers de configuration des équipements.
- ☐Des schémas de repérage de l'installation sont créés ou complétés.
- ☐Un reporting régulier (avancement, points d'étapes, alertes) au client, à la hiérarchie, aux prestataires est effectué.

Le style, le ton et la terminologie utilisés sont adaptés à la personne et aux circonstances
Le travail est effectué selon les attentes exprimées de temps, de quantité ou de qualité
Le travail est préparé de façon à satisfaire les exigences de qualité, d'efficacité et d'échéancier

C11 : MAINTENIR UN RÉSEAU INFORMATIQUE

Les outils logiciels et matériels permettant d'effectuer les tests et l'analyse du système d'information sont identifiés et mis en œuvre selon les spécifications

- ☐Les outils logiciels et matériels de test sont identifiés.
- ☐Les tests sont réalisés dans un ordre logique.
- ☐Les tests sont réalisés sans oublis.
- ☐Le rapport d'incident est complété avec les résultats.

Les résultats de tests et d'analyse sont interprétés de manière pertinente et les causes de l'incident sont localisées

- ☐La correspondance outils utilisés / diagnostiques est présentée.
- ☐Les résultats des tests sont correctement lus, le niveau de criticité est établi.
- ☐Les causes sont localisées, la durée du diagnostic est optimale.
- ☐Les procédures de traitement de l'incident sont choisies et réalisées.

L'incident est résolu ou qualifié et escaladé, le service est opérationnel

- ☐La remise en service est effective, les vérifications de l'état du système sont effectuées.
- ☐Une fiche de clôture d'incident est complétée.
- ☐ Si l'incident demande l'intervention d'un expert, les tests et les causes probables sont succinctement expliqués dans une fiche de suivi d'incident. Si l'incident incombe au technicien, les actions à mener sont identifiées et réalisées.
- ☐Une fiche pour la base de connaissance de l'entreprise peut être proposée.

Le client est correctement informé et conseillé quant aux mesures de prévention possibles

- ☐Le client est informé des causes de l'incident.
- ☐Le client est informé des mesures de prévention à suivre.
- ☐Le client est informé des actions à mener pour éviter la reproduction de l'incident.
- ☐Des outils de surveillances, des scripts d'alertes sont proposés.

Le style, le ton et la terminologie utilisés sont adaptés à la personne et aux circonstances
Les risques d'une situation de travail sont repérés et les mesures appropriées pour sa santé, sa sécurité et celle des autres sont adoptées
Face à un ensemble de faits, des actions appropriées à poser sont décidées