

Procédure de Gestion des Incidents Informatiques

1. Introduction

Cette procédure décrit les étapes à suivre pour gérer efficacement les incidents informatiques afin de minimiser l'impact sur les opérations de l'entreprise et d'assurer une résolution rapide.

2. Objectifs

- Détection rapide des incidents.
- Réponse efficace pour minimiser l'impact.
- Restauration rapide des services affectés.
- Prévention des futurs incidents par l'analyse des causes.

3. Définition des Termes

- Incident : Événement imprévu perturbant un service informatique.
- Impact : Effet de l'incident sur les opérations.
- Urgence : Vitesse nécessaire pour résoudre l'incident.
- Priorité : Importance de l'incident basée sur son impact et son urgence.

4. Rôles et Responsabilités

- Équipe de support : Premier point de contact pour la détection et l'enregistrement des incidents.
- Gestionnaire des incidents : Responsable de la coordination de la réponse.
- Équipes techniques : Responsable du diagnostic et de la résolution.
- Direction : Informée des incidents critiques et impliquée dans la revue post-incident.

5. Étapes de la Gestion des Incidents

Procédure de Gestion des Incidents Informatiques

5.1. Détection et Enregistrement

- Surveillance continue : Utiliser des outils de surveillance pour détecter les anomalies.
- Signalement manuel : Les utilisateurs signalent les incidents via un portail ou en contactant le support.
- Enregistrement : Saisir tous les détails de l'incident dans le système de gestion des incidents.

5.2. Classification et Priorisation

- Évaluation : Déterminer l'impact et l'urgence de l'incident.
- Priorisation : Attribuer une priorité (critique, haute, moyenne, basse).

5.3. Diagnostic

- Analyse : Identifier la cause profonde de l'incident.
- Documentation : Enregistrer les étapes de diagnostic.

5.4. Résolution et Restauration

- Plan de résolution : Développer un plan pour résoudre l'incident.
- Mise en œuvre : Appliquer les correctifs.
- Tests : Vérifier que la solution fonctionne et que le service est restauré.

5.5. Clôture

- Vérification : Assurer que toutes les actions nécessaires ont été complétées.
- Documentation : Compléter le rapport d'incident.
- Communication : Informer les parties prenantes de la résolution.

5.6. Revue Post-Incident

Procédure de Gestion des Incidents Informatiques

- Analyse approfondie : Examiner les incidents majeurs.
- Amélioration continue : Utiliser les leçons tirées pour prévenir les futurs incidents.

6. Outils et Ressources

- Logiciel de gestion des tickets : Pour enregistrer et suivre les incidents.
- Outils de surveillance : Pour détecter les anomalies.
- Base de connaissances : Pour documenter les solutions et les meilleures pratiques.

7. Communication

- Notification des parties prenantes : Informer régulièrement les parties prenantes sur l'état de l'incident et les actions entreprises.
- Mises à jour régulières : Fournir des mises à jour sur la progression de la résolution.

8. Annexe

Annexe A : Modèle de Rapport d'Incident

1. Identifiant de l'incident : [Numéro unique]
2. Date et heure de détection : [Date et heure]
3. Signalé par : [Nom de l'utilisateur ou du système]
4. Description de l'incident : [Détails de l'incident]
5. Systèmes affectés : [Liste des systèmes]
6. Évaluation de l'impact : [Description de l'impact sur les opérations]
7. Urgence : [Critique/Haute/Moyenne/Basse]
8. Actions de diagnostic : [Étapes prises pour diagnostiquer l'incident]

Procédure de Gestion des Incidents Informatiques

9. Cause identifiée : [Description de la cause]
10. Plan de résolution : [Actions prévues pour résoudre l'incident]
11. Actions entreprises : [Détails des actions prises]
12. Résultats des tests : [Résultats des vérifications post-résolution]
13. Date et heure de clôture : [Date et heure]
14. Leçons apprises : [Détails des leçons tirées]
15. Recommandations : [Suggestions pour éviter de futurs incidents]

Annexe B : Matrice de Priorisation des Incidents

Impact	Urgence	Priorité	Description
Critique	Haute	1	Impact majeur sur les opérations essentielles.
Critique	Moyenne	2	Impact majeur mais peut attendre une courte période.
Critique	Basse	3	Impact majeur mais sans urgence immédiate.
Haute	Haute	2	Impact significatif nécessitant une attention rapide.
Haute	Moyenne	3	Impact significatif mais peut attendre un peu.