|  |
| --- |
| [organisation / département / unité opérationnelle] |
| Plan de continuité des activités avec accent mis sur les dépendances informatiques critiques |
|  |
| **Holland, Tilly** |
| **Révisé et testé le - [Choisissez la date]** |
|  |

|  |
| --- |
| *[Tapez le récapitulatif du document ici. Le récapitulatif est généralement un bref résumé du contenu du document.]* |

# **À propos de ce modèle**

*L’objet de ce modèle est de permettre aux petites entreprises de se familiariser avec les blocs de construction de la planification de continuité des activités/reprise après sinistre (BCP/DR), et de commencer à penser à ce qu’il serait nécessaire de faire pour reprendre une activité normale si leurs données et infrastructures venaient à subir une catastrophe informatique.*

*Chaque organisation utilise l’informatique différemment, c’est pourquoi il n’existe pas de plan de continuité des activités ou de reprise après sinistre universel pouvant être appliqué à toutes les organisations. Néanmoins, les stratégies BCP/DR les plus efficaces suivent toutes une approche similaire :*

* *Qu’est-ce qui est important et que nous pouvons réaliser/livrer*
* *De quoi dépendons-nous pour parvenir à ceci ?*
  + *Dans ce modèle, nous nous concentrons uniquement sur les ressources informatiques essentielles*
* *Sommes-nous suffisamment robustes ?*
* *Comment réagir si les choses ne se déroulent pas comme prévu ?*

*Afin de simplifier le travail de planification, vous devez planifier pour chaque « niveau », par ex. clarifier les besoins et dépendances au niveau de l’entreprise, du service informatique et de la salle des serveurs. Dans ce modèle nous mettons l’accent sur les petites entreprises, qui prennent les premières mesures dans le domaine, d’autres modèles plus détaillés pouvant être utilisés par la suite lorsque le contexte de ce modèle est assimilé. Pour plus d’informations, veuillez contacter votre représentant Ontrack local.*

# **Introduction**

Ce document détaille les politiques et procédures de [organisation / département / unité opérationnelle] dans le cas d’une interruption des services informatiques critiques ou d’une détérioration des équipements informatiques ou des données. Ces processus garantiront que ces actifs sont récupérables au niveau adéquat et dans les délais nécessaires pour permettre de reprendre une activité normale avec un impact minimal sur l’entreprise.

Notre mission est de garantir le fonctionnement des systèmes d’information, l’intégrité et la disponibilité des données, ainsi que la continuité des activités.

# **Déclaration de politique**

La gestion des entreprises a approuvé la déclaration de politique suivante :

* La société doit mettre en œuvre un plan de continuité et de récupération adéquat.
* Tous les plans de continuité et de récupération doivent couvrir les éléments, systèmes et réseaux d’infrastructure essentiels, en conformité avec les activités clés de l’entreprise.
* Les plans doivent être testés de façon périodique dans un environnement simulé afin de garantir qu’ils peuvent être mis en œuvre dans les situations d’urgence et que la direction et le personnel comprennent comment ils doivent être exécutés.
* L’ensemble du personnel doit être sensibilisé sur les plans et les rôles de chaque employé.
* Les plans de continuité et de récupération doivent être actualisés afin qu’ils prennent en compte l’évolution des circonstances.

**Analyse de l’impact sur les activités**

Ci-dessous, une analyse simplifiée de l’impact sur les activités à utiliser lorsque vous effectuez le travail de planification pour la première fois.

La première section concerne l’identification des services informatiques importants nécessaires aux activités ainsi que l’impact sur les activités si celles-ci sont interrompues. La deuxième section concerne l’identification des besoins opérationnels en matière de disponibilité, de temps de récupération, de sauvegarde, ainsi que d’intégrité et de confidentialité des données.

|  |  |  |
| --- | --- | --- |
| **Processus opérationnel/exécution des opérations** | **Service informatique** | **Impact lorsqu’interrompu, y compris le moment où cela devient inacceptable** |
| *Production en usine* | *Système informatique A* | *Les chaînes de montage s’arrêteront immédiatement, inacceptable après 4 heures* |
|  |  |  |
| *Finances* | *Système informatique B* | *La création de factures et de rapports sera arrêtée immédiatement, inacceptable après 24 heures* |
|  |  |  |
| *RH* | *Système informatique C*  *Système informatique B* | *Signifiera l’utilisation de procédures manuelles préparées, inacceptable après 48 heures* |
|  |  |  |
| *Tout le personnel de l’entreprise* | *Système email* | *Impactera la productivité immédiatement, inacceptable après 4 heures* |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Service informatique** | **Besoin opérationnel de :** | |  |  |  | | |  |
|  | **Disponibilité** | **DMIA** | | **PDMA** | | **Intégrité des données** | **Confidentialité des données** | |
| *Système informatique A* | *99,7 %* | *4 h* | | *10 min* | | *Très élevée* | *Faible* | |
| *Système informatique B* | *99,5 %* | *24 h* | | *24 h* | | *Très élevée* | *Élevée* | |
| *Système informatique C* | *99,5 %* | *48 h* | | *24 h* | | *Très élevée* | *Très élevée* | |
| *Système email* | *99,9 %* | *4 h* | | *12 h* | | *Très élevée* | *Moyenne* | |

La Durée maximale d’interruption admissible (DMIA) est le laps de temps convenu pour que le processus opérationnel et l’exécution des opérations fonctionnent de nouveau après une interruption informatique (y compris toutes les actions de récupération informatique).

La Perte de données maximale admissible (PDMA) est la quantité acceptable de données que vous pouvez perdre dans un incident sans être en mesure de les récupérer. Récupération à partir d’un « point dans le temps » ultérieur. Définit les demandes en solutions de sauvegarde/restauration/réplication.

L’intégrité des données est l’exigence concernant ces informations que celles-ci restent intactes et ne sont pas modifiées, que ce soit de façon intentionnelle ou non intentionnelle.

La confidentialité des données est l’exigence concernant ces informations que celles-ci ne soient pas rendues accessibles ni dévoilées, que ce soit de façon intentionnelle ou non intentionnelle, à d’autres personnes.

**Analyse de robustesse**

Lorsque les besoins / exigences opérationnels en ressources informatiques importantes sont identifiés, vous devez effectuer une analyse pour déterminer si vous avez le niveau de robustesse adéquat pour soutenir votre entreprise. À noter que ceci inclut si le vôtre est trop faible (un risque) ou trop élevé (un coût).  
  
Contactez la personne responsable de chaque service informatique concerné pour le travail de planification et ayez une discussion approfondie concernant les besoins opérationnels et ce qui est pris en charge aujourd’hui. Au final, il s’agit d’une décision d’entreprise quant à ce qui doit être mis en place, y compris quels risques l’entreprise est prête à prendre si par ex. le coût d’un service informatique plus performant est trop élevé. Utilisez le tableau ci-dessous pour décrire les actions identifiées.

|  |  |  |
| --- | --- | --- |
| **Action** | **Description** | **Plan de mise en œuvre** |
| *Changer la solution de sauvegarde* | *Identifier une nouvelle solution pour le système informatique A afin de répondre aux besoins opérationnels de la Perte de données maximale admissible* | *Analyse faite le (date)* |
| *DMIA système email* | *Discuter du coût d’une Durée maximale d’interruption admissible plus courte avec le fournisseur* | *Discussion (date)* |
| *Effacement sécurisé de tous les disques durs lorsqu’ils sont remplacés* | *Discuter d’une solution avec Ontrack afin d’effacer tous les disques durs de façon sécurisée lorsqu’ils sont remplacés (pour tous les systèmes avec une exigence de confidentialité élevée ou très élevée)* | *Discussion (date)* |

**Section planification de la récupération**

Cette partie du Plan de continuité des activités couvre les préparations permettant de développer une capacité de gérer une interruption informatique de façon efficace et de réduire l’impact sur les activités.

**Informations de contact clés**

| **Nom, Titre** | **Option de contact** | **Numéro de contact** |
| --- | --- | --- |
| **Nom 1** | Travail |  |
| Système informatique A | Mobile |  |
|  | Domicile |  |
|  | Adresse email |  |
|  |  |  |
| **Nom 2** | Travail |  |
| Système informatique B | Mobile |  |
|  | Domicile |  |
|  | Adresse email |  |
|  |  |  |
| **Nom 3** | Travail |  |
| Système informatique C | Mobile |  |
|  | Domicile |  |
|  | Adresse email |  |
|  |  |  |
| **Nom 4** | Travail |  |
| Salle des serveurs locale | Mobile |  |
|  | Domicile |  |
|  | Adresse email |  |
|  |  |  |
|  | Travail |  |
|  | Mobile |  |
|  | Domicile |  |
|  | Adresse email |  |
|  |  |  |
|  | Travail |  |
|  | Mobile |  |
|  | Domicile |  |
|  | Adresse email |  |

# **Contacts externes**

| **Nom, titre** | **Option de contact** | | **Numéro de contact** |
| --- | --- | --- | --- |
| **Propriétaire / Gestionnaire immobilier** |  | |  |
| Numéro de compte |  | |  |
|  | Travail | |  |
|  | Mobile | |  |
|  | Domicile | |  |
|  | Adresse email | |  |
|  |  | |  |
| **Fournisseur d’énergie** |  | |  |
| Numéro de compte | Travail | |  |
|  | Mobile | |  |
|  | Domicile | |  |
|  | Adresse email | |  |
|  |  | |  |
| **Opérateur télécom** |  | |  |
| Numéro de compte | Travail | |  |
|  | Mobile | |  |
|  | Fax | |  |
|  | Domicile | |  |
|  | Adresse email | |  |
|  |  | |  |
| **Récupération des données - Ontrack** |  | |  |
| Numéro de compte | Travail | |  |
|  | Mobile | |  |
|  | Domicile | |  |
|  | Adresse email | |  |
|  |  | |  |
| **Fournisseur de matériel informatique 1** |  | |  |
| Numéro de compte | Travail | |  |
|  | Mobile | |  |
|  | Rapports d’urgence | |  |
|  | Adresse email | |  |
|  |  | |  |
| **Fournisseur de serveurs 1** |  | |  |
| Numéro de compte | Travail | |  |
|  | Mobile | |  |
|  | Fax | |  |
|  | Adresse email | |  |
|  |  | |  |
| **Fournisseur d’email** |  |  | |
| Numéro de compte | Travail |  | |
|  | Mobile |  | |
|  | Domicile |  | |
|  | Adresse email |  | |
|  |  |  | |

**Procédures de récupération de données préparées**

En fonction de l’incident, au moins l’une des procédures de *reprise après sinistre* suivantes peut être déclenchée :

## Plan de récupération de données pour les ransomware

|  |  |
| --- | --- |
| **Scénario** | Ransomware détecté sur un ou plusieurs ordinateurs/serveurs |
| **Causes possibles** | Malware |
| **Services informatiques et données à risques** | Système de stockage et ordinateurs portables |
| **Impact** | Données perdues ou corrompues |

|  |  |
| --- | --- |
| **Prévention** | * Mettre en place un système d’emails sécurisés pour éviter les emails de phishing * Sécuriser votre réseau et votre environnement informatique * Former les employés * Utiliser un VPN pour accéder au protocole Remote Desktop de votre organisation, ceci permettant de créer une connexion sécurisée entre les employés de l’organisation et Internet. * S’assurer qu’une authentification à deux facteurs est configurée * Les employés faisant fonctionner des services internes importants doivent disposer de l’accès maximum requis pour effectuer leur mission. Tout employé ayant accès aux systèmes ou sauvegardes critiques doit avoir une authentification à deux facteurs configurée * Mettre en place un plan de sauvegarde et de récupération pour toutes les données critiques avec la stratégie 3-2-1 :   + 3 – Conserver un minimum de trois copies des données 2 – Stocker les données sur deux types de supports différents 1 – Sécuriser une copie de vos sauvegardes hors site * Tester les sauvegardes de façon régulière afin de garantir une bonne configuration, ce qui limitera l’impact d’une fuite de données et accélèrera le processus de récupération * Isoler les sauvegardes critiques du réseau (air gap) pour une protection maximale * Mettre en œuvre des systèmes de fichiers de type copy-on-write (NetApp WAFL – Linux ZFS) ou des fonctions WORM dans les systèmes ou dispositifs NAS * Appliquer les correctifs des systèmes d’exploitation critiques et logiciels antivirus, de sécurité et de sauvegarde dès que possible * Mettre en place une formation continue sur la cybersécurité pour les utilisateurs et administrateurs en vue d’identifier les emails de phishing |

|  |  |
| --- | --- |
| **Plan d’action** | * Déconnecter tout matériel affecté en débranchant le câble réseau * Ne jamais payer la rançon ! Accéder à la requête des malfaiteurs ne garantit pas que vous récupérerez vos données. Très souvent, et très certainement s’il s’agit d’un ranscam ou d’un malware wiper, vous ne récupérerez pas vos données, et vous vous retrouverez sans données et avec un gouffre dans vos finances * Ne pas essayer de déchiffrer les données vous-même. Certains spécialistes en informatique peuvent avoir les compétences pour récupérer les données perdues, mais c’est risqué. Si les choses se déroulent mal, vous pourriez détruire vos données pour toujours * Vérifier votre sauvegarde. Même si votre sauvegarde est manquante après une attaque ransomware, n’excluez jamais la possibilité d’une récupération. Les solutions possibles dépendent du type de support ou du système de stockage, ainsi que du type de ransomware * Identifier le problème, coordonner une réponse initiale (Jane Doe) * Demander des conseils immédiatement en contactant Ontrack * Suivre les instructions dans le détail |

|  |  |
| --- | --- |
| **Contacts clés** | * John Smith (administrateur des systèmes informatiques) * Stuart Burrows (contact Ontrack) * Jane Doe (responsable des installations) |

## 

## Plan de récupération de données pour les systèmes virtualisés

|  |  |
| --- | --- |
| **Scénario** | Situation de perte de données dans les systèmes virtuels |
| **Causes possibles** | * Le manque de temps : Régulièrement, un employé informatique manque du temps nécessaire pour documenter les procédures et processus * Continuer à travailler sur un serveur touché après qu’une suppression des données s’est produite * Pannes mécaniques et problèmes liés au système RAID et/ou au stockage * Machine virtuelle/VMDK supprimée ou manquante * Métadonnées VMFS corrompues ou entrepôt de données inaccessible * Corruption à l’intérieur de l’OS invité * Les processus de sauvegarde des données sont obsolètes |
| **Services informatiques et données à risques** | Systèmes de stockage virtuels |
| **Impact** | Données perdues ou corrompues |

|  |  |
| --- | --- |
| **Plan d’action** | * Faire en sorte que les employés aient suffisamment de temps pour sauvegarder les données * Ne jamais travailler sur un serveur touché lorsqu’une suppression des données s’est produite * S’assurer que tous les processus de sauvegarde sont actualisés et avoir un plan d’urgence en place en cas de perte de données * Restaurer les données vers un autre système * Ne jamais réutiliser le disque reconstruit. Les nouveaux fichiers ou machines virtuelles ne doivent pas être créés avant que les données aient été restaurées * Ne pas exécuter les outils de réparation des systèmes de fichiers FSCK ou CHKDSK sur un disque virtuel, à moins qu’une bonne sauvegarde ait été validée en la restaurant vers un volume différent * S’assurer d’avoir un plan de contingence à jour avec les meilleures pratiques en matière de récupération des données et les informations de contact d’experts reconnus |

|  |  |
| --- | --- |
| **Contacts clés** | * John Smith (administrateur des systèmes informatiques) * Stuart Burrows (contact Ontrack) * Jane Doe (responsable des installations) |

# 

## Plan de récupération de données pour les systèmes RAID

|  |  |
| --- | --- |
| **Scénario** | Situation de perte de données dans les systèmes RAID |
| **Causes possibles** | * Erreur humaine   + Que ce soit à cause d’un accident ou d’une intention malveillante, une perte de données suite à un reformatage, à la réinstallation ou à l’écrasement d’un volume, des ingénieurs experts en récupération des données peuvent y remédier * Problèmes d’alimentation   + Les systèmes RAID peuvent être affectés par une perte de puissance, une mise hors tension et une surtension entraînant une perte de données. Les systèmes RAID fonctionnant dans un état dégradé sont particulièrement vulnérables, les problèmes d’alimentation pouvant entraîner une désynchronisation des lecteurs devant être réintégrés dans la matrice * Problèmes mécaniques et reconstructions défectueuses   + Les systèmes RAID sont conçus pour résister à une panne d’un lecteur individuel, mais une fois qu’un système RAID fonctionne dans un état dégradé, la charge de travail des lecteurs restants augmente, de même que le risque de panne des lecteurs restants. Une panne sur l’un des lecteurs restants peut entraîner une panne généralisée du système RAID * Catastrophes naturelles   + Le feu, l’eau, la poussière ainsi que d’autres contaminants provenant de catastrophes naturelles peuvent détruire plusieurs lecteurs instantanément |
| **Services informatiques et données à risques** | Systèmes RAID |
| **Impact** | Données perdues ou corrompues |

|  |  |
| --- | --- |
| **Plan d’action** | * Ne pas exécuter CHKDSK   + Tandis que CHKDSK peut s’avérer utile sur les systèmes à lecteur unique avec une légère corruption pour forcer les systèmes de fichiers à rester dans un état constant, dans la plupart des cas, les incohérences dans un volume stocké sur un système RAID sont le résultat de problèmes au niveau du RAID (c.-à-d. des lecteurs désynchronisés, une mauvaise reconstruction, etc.). Exécuter CHKDSK dans ces scénarios précis peut entraîner des dommages irréversibles aux structures des systèmes de fichiers * Ne jamais remplacer un lecteur défectueux par un lecteur faisant partie d’un système RAID précédent ;   + Toujours réinitialiser le lecteur de remplacement avant de l’utiliser * Si un lecteur produit des sons mécaniques inhabituels, il doit être mis hors tension immédiatement   + Un lecteur mécaniquement défectueux qui est encore utilisé peut accroître la gravité de la perte de données et réduire les chances d’une récupération complète * Créer et vérifier une sauvegarde de données sur un système RAID avant d’effectuer des modifications matérielles ou logicielles * Étiqueter les lecteurs avec leur position dans une matrice RAID avant de les retirer de votre système * Si un système RAID tombe en panne au milieu d’un processus de reconstruction, ne pas effectuer d’autres tentatives de reconstruction * Dans une situation de perte de puissance avec une matrice RAID, si le système de fichiers paraît suspect, ne peut être monté, ou si les données sont inaccessibles après un retour à la normale de l’alimentation, ne pas exécuter d’utilitaires de réparation de volume |

|  |  |
| --- | --- |
| **Contacts clés** | * John Smith (administrateur des systèmes informatiques) * Stuart Burrows (contact Ontrack) * Jane Doe (responsable des installations) |

## Plan de récupération de données pour HDD et SSD simples

|  |  |
| --- | --- |
| **Scénario** | Situation de perte de données dans les lecteurs uniques |
| **Causes possibles** | * Pannes mécaniques   + Si votre disque dur ne fonctionne pas et/ou produit des sons de cliquetis ou de grincements, cela signifie qu’il subit une panne mécanique. Ceci peut être dû au plantage de la tête de lecture et/ou à une panne du moteur * Pannes logiques   + Si votre disque dur fonctionne mais que vous ne pouvez accéder à une partie ou à l’ensemble de vos fichiers, cela signifie qu’il subit une panne logique. Ceci peut être dû à une partition perdue ou à un reformatage accidentel du lecteur |
| **Services informatiques et données à risques** | Données d’utilisateur stockées localement sur un lecteur unique |
| **Impact** | Données perdues |

|  |  |
| --- | --- |
| **Plan d’action** | * Mise hors tension   + Mettre votre ordinateur ou votre appareil de stockage hors tension afin de prévenir tout dommage supplémentaire * Dégât des eaux   + NE PAS FAIRE SÉCHER. La corrosion d’un support commence avec le séchage et accroît les risques de perte de données. Placer le disque dur dans un sac à fermeture hermétique et l’envoyer dès que possible à un bureau Ontrack pour une récupération des données du disque dur * Sons inhabituels   + Mettre hors tension. Si votre disque dur produit des sons de cliquetis ou de grincements, c’est un signe que votre lecteur a subi un plantage de la tête de lecture et qu’il ne lit plus les données correctement. Un plantage de la tête de lecture peut entraîner des dommages irréparables à vos fichiers si le lecteur continue à fonctionner * Fichiers manquants, reformatés ou supprimés   + Qu’il s’agisse d’une suppression accidentelle ou que vos fichiers soient manquants, notre logiciel de récupération des données à utiliser soi-même peut être votre solution. Téléchargez une version d’essai gratuite du logiciel pour obtenir la liste des fichiers récupérables. Si les fichiers que vous recherchez sont récupérables, il vous suffit d’acheter la licence pour télécharger les données |

|  |  |
| --- | --- |
| **Contacts clés** | * John Smith (administrateur des systèmes informatiques) * Stuart Burrows (contact Ontrack) * Jane Doe (responsable des installations) |

## Historique des révisions

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Détails des révisions** |
|  |  |  |