

prÉrequis HOP’EN

PLAN DE REPRISE D’ACTIVITÉ DU SI
ET PROCÉDURES DE FONCTIONNEMENT
EN MODE DÉGRADÉ
DE L’ÉTABLISSEMENT xxx

**[Date]**

Sommaire

[1. Objet 2](#_Toc10540794)

[2. Responsabilités 2](#_Toc10540795)

[3. Description 3](#_Toc10540796)

[3.1. Infrastructure fonctionnelle 3](#_Toc10540797)

[3.2. Dispositions prévues pour la récupération des données 5](#_Toc10540798)

[3.3. Dispositions prévues pour le fonctionnement des applications en mode dégradé et le retour à la normale 6](#_Toc10540799)

[3.4. Dispositions prévues pour le redémarrage des applications 6](#_Toc10540800)

[3.5. Information des utilisateurs en cas de panne 7](#_Toc10540801)

[3.6. Pour aller plus loin 7](#_Toc10540802)

# Objet

Le présent documenta pour objectif de décrire le sommaire du Plan de Reprise d’Activité (PRA) du système d’information du *[Nom de l’établissement de santé]*. Le document liste le minimum de dispositions que doit prévoir l’établissement pour assurer la reprise de l’activité de son système d’information en cas de crise majeure ou importante du centre informatique.

Ce document présente les questions à se poser relatives aux points suivants :

* **Les applications « métier » exploitées par l’établissement de santé**;
* **Le plan de sauvegarde des données contenues dans le système d’information de l’établissement ;**
* **Les procédures de fonctionnement des applications en mode dégradé (en cas de dysfonctionnements) et les procédures de retour à la normale ;**
* **Les modalités de redémarrage du système d’information en cas de panne** ;
* **L’information des utilisateurs**

# Responsabilités

|  |
| --- |
| Cette section vise à décrire les responsabilités pour la bonne mise en application du Plan d’activité d’Activité et son suivi.Elle peut prendre la forme d’une matrice de responsabilité afin de décrire précisément les rôles et contributions de chaque acteur sur chaque étape. |

# Description

## Infrastructure fonctionnelle

###  Présentation de l’architecture applicative

|  |
| --- |
| Cette section vise à décrire le patrimoine applicatif de l’établissement de santé. La cartographie applicative du système d’information pourra ainsi être intégrée ici. Par ailleurs, l’établissement pourra s’appuyer sur les travaux qui auront été menés dans le cadre du programme HOP’EN sur la cartographie applicative pour compléter ce paragraphe *(c.-à-d. indicateur P1.1. Taux d’application au cœur du processus de soins, de la gestion administrative du patient et du PMSI connectées à un référentiel unique d’identités des patients)*. |

### Classification des applications exploitées

Cette section indique pour chaque application exploitée par l’établissement de santé son niveau de disponibilité et si celle-ci est externalisée ou non. Les applications sont organisées dans le tableau ci-dessous par domaine fonctionnel. Les informations suivantes seront notamment renseignées dans le tableau ci-dessous :

 – Domaine : nom du domaine fonctionnel auquel appartient l’application décrite ;

 – Fonctionnalité : nom de la fonctionnalité à laquelle appartient l’application décrite ;

 – Application : nom de l’application décrite ;

 – Éditeur : nom de l’éditeur de l’application décrite ;

 – Besoin en disponibilité : besoin en disponibilité de l’application décrite sur une échelle de 1 à 4 (cf. fiche pratique 4 du présent document) ;

 – Externalisation : indiquer si l’application décrite est externalisée ou non (Oui/Non)

Une illustration est proposée ci-dessous afin d’aider l’établissement à renseigner le tableau.

L’établissement de santé pourra par ailleurs s’appuyer sur les travaux qui auront été menés dans le cadre du programme HOP’EN sur la mesure du taux de disponibilité des applications pour compléter ce tableau *(c.-à-d. indicateur P2.2. Définition d’un taux de disponibilité cible des applicatifs et mise en œuvre d’une évaluation de ce taux)*.

Enfin, il pourra être ajouté dans la présente section toute information relative aux applications exploitées qui sera jugée pertinente par l’établissement de santé.

*[Indiquer le nom de l’établissement de santé]*exploite les applications listées dans le tableau ci-dessous. Pour chacune de ces applications, classées par domaine fonctionnel, sont précisés le besoin de disponibilité et l’éventuelle externalisation de celle-ci.

Les domaines fonctionnels indiqués dans le tableau ci-dessous sont ceux utilisés dans l’observatoire des Systèmes d’Information Hospitaliers oSIS.

| **Domaine**  | **Fonctionnalité** | **Application** | **Éditeur** | **Besoin en Disponibilité** | **Externalisation** |
| --- | --- | --- | --- | --- | --- |
| ***Gestion administrative du patient***  |  | Application A | Editeur A | Sur une échelle de 1 à 4 | Oui |
|  | Application B | Editeur B | Sur une échelle de 1 à 4 | Non |
| ***Gestion du dossier patient (médical et paramédical)*** |  |  |  |  |  |
|  |  |  |  |  |
| ***Gestion des resources*** |  |  |  |  |  |
|  |  |  |  |  |
| ***Gestion des prescriptions et demandes d’examens*** |  |  |  |  |  |
|  |  |  |  |  |
| ***Gestion des activités médico-techniques*** |  |  |  |  |  |
| ***Urgences*** |  |  |  |  |  |
|  |  |  |  |  |
| ***Recueil d’activités, production des données T2A*** |  |  |  |  |  |
|  |  |  |  |  |
| ***Système d’information économique et financier*** |  |  |  |  |  |
|  |  |  |  |  |
| ***Système d’information logistique et technique*** |  |  |  |  |  |
|  |  |  |  |  |
| ***Gestion des identités*** |  |  |  |  |  |
|  |  |  |  |  |
| ***Gestion des Ressources Humaines*** |  |  |  |  |  |
|  |  |  |  |  |
| ***Système d’information Qualité et Gestion des risques*** |  |  |  |  |  |
|  |  |  |  |  |
| ***Système d’information de pilotage***  |  |  |  |  |  |
|  |  |  |  |  |
| ***Système d’information de Réseau Ville – Hôpital/Hôpital – Hôpital*** |  |  |  |  |  |
|  |  |  |  |  |
| ***[Nom du domaine fonctionnel]*** |  |  |  |  |  |
|  |  |  |  |  |

Cette liste permet avant tout, sur la base des besoins en disponibilité, de définir un ordre de priorité dans le redémarrage des applications. Ensuite, pour affiner l’ordre de redémarrage, il faut prendre en compte les interactions et dépendances entre applications.

## Dispositions prévues pour la récupération des données

Cette section décrit les mécanismes prévus par la structure — et le cas échéant, les sociétés en charge de l’hébergement, de l’exploitation et de la maintenance du système d’information de la structure — pour permettre la restauration des données du système d’information suite à un incident.

### Plan de sauvegarde des données

L’établissement définit tout d’abord le plan de sauvegarde des données contenues dans le système d’information. Pour ce faire, il pourra s’appuyer sur le tableau ci-dessous qui recense les informations suivantes :

 – Plateforme : nom de la plateforme de sauvegarde des données ;

 – Type de plateforme : type de plateforme de sauvegarde des données ;

 – Type de sauvegarde (incrémentale/totale) : sauvegarde des données distinctes par rapport à la précédente sauvegarde uniquement/sauvegarde de l’ensemble des données ;

 – Planification (incrémentale/totale) : périodicité, jour et heure de la sauvegarde des données.

Afin de renseigner ce tableau, l’établissement de santé pourra se référer aux engagements contractuels des sociétés en charge de la maintenance du système d’information pour recueillir ces informations.

La sauvegarde des données contenues dans le système d’information de l’établissement est placée sous la responsabilité de *[nom de l’établissement/nom des sociétés en charge de la maintenance du système d’information ou nom de la personne de l’établissement].*

Les dispositifs de sauvegarde des données détenues par l’établissement sont ici décrits :

* *[Présenter ici les dispositifs de sauvegarde dont dispose l’établissement de santé (exemples : boitier de sauvegarde, robot…)] ;*

Le tableau ci-dessous présente le plan de sauvegarde des données de l’établissement :

| **Plateforme** | **Type de plateforme** | **Type de sauvegarde** | **Planification de la sauvegarde des données** | **Planification des tests de Restauration des données** |
| --- | --- | --- | --- | --- |
| ***Incrémentale*** | ***Totale*** | ***Incrémentale*** | ***Totale*** | ***Incrémentale*** | ***Totale*** |
| ANAPATH2 | Windows serveur 2003 | Totales\_VLS2 | Incrémentales\_VLS | 3 fois par jour8 h – 12 h – 20 h | Tous les vendredis 20 h 30 | Tous les mois | Tous lesmois |

### Procédures de récupération des données

Une fois le plan de sauvegarde des données élaboré, l’établissement élabore les procédures de récupération des données en fonction des types de sauvegarde qui auront été définis préalablement dans le plan de sauvegarde (c.-à-d. sauvegarde incrémentale ou sauvegarde totale).

Ces procédures précisent notamment les points suivants :

 – Diagnostic de la perte de données : nature et volume des données perdues, ampleur et gravité de la perte… ;

 – Détermination des données à récupérer en fonction des données perdues et des sauvegardes disponibles : définir parmi les sauvegardes existantes celles à restaurer (par exemple la dernière sauvegarde incrémentale, ou restauration complète en reprenant la dernière sauvegarde totale suivie des sauvegardes incrémentales)

 – Mode de mise en œuvre de la récupération des données : actions à mener, délai de réalisation, tests de vérification de la bonne récupération des données prévues… ;

 – Modalités d’information des utilisateurs : nature de l’information communiquée (données perdues/sauvegardées/récupérées), support de communication utilisé, durée estimée de la perte de données…

Les procédures de récupération des données devront être élaborées en tenant compte des dispositions du plan de sauvegarde des données qui aura été défini au préalable par l’établissement de santé.

Les procédures de récupération et de sauvegarde doivent être testées périodiquement.

## Dispositions prévues pour le fonctionnement des applications en mode dégradé et le retour à la normale

Procédures de fonctionnement en mode dégradé et de retour à la normale du système d’information prévues par l’établissement de santé. (Voir l’annexe Procédures de fonctionnement en mode dégradé/de retour à la normale du système d’information).

## Dispositions prévues pour le redémarrage des applications

Cette section présente la procédure retenue par l’établissement de santé pour permettre le redémarrage en cas de dysfonctionnement des applications qu’il exploite.

L’établissement de santé inclura notamment dans cette procédure les points suivants :

 – Le diagnostic du (des) dysfonctionnement(s) ayant entraîné une panne des applications ;

 – Les modalités de redémarrage : restauration des données puis redémarrage des applications, dans un ordre défini, en fonction des priorités (selon les besoins en disponibilité) et des indications données par les éditeurs des solutions exploitées. Empêcher par exemple toute connexion au système par les utilisateurs durant la durée de l’intervention.

 – La vérification du bon fonctionnement des applications : procédure de vérification à prévoir dans l’environnement de production avant d’informer les utilisateurs que les applications sont de nouveau disponibles (ce n’est pas une procédure de tests qui elle se fait dans un environnement de test, mais une procédure de vérification qui garantisse que toutes les fonctions sont rétablies en production)

## Information des utilisateurs en cas de panne

Cette section définit la procédure d’information des utilisateurs en cas de panne du système d’information qui aura été défini par l’établissement de santé

Cette procédure s’articule notamment autour des points suivants :

 1. Information des utilisateurs de l’indisponibilité du système d’information

 Ce point précise les informations qui seront communiquées aux utilisateurs en cas d’indisponibilité du système d’information de l’établissement : la nature du dysfonctionnement rencontré, les ressources informatiques indisponibles, la durée de leur indisponibilité, la date prévisible de la résolution du dysfonctionnement…

 Il précise également le support de communication de cette information aux utilisateurs (exemples : messagerie électronique, téléphone, note de service…

 2. Information des utilisateurs de la reprise d’activité du système d’information

 Ce point de la procédure a pour objectif de préciser l’information communiquée aux utilisateurs lors de la reprise d’activité du système d’information : les modalités de résolution du dysfonctionnement, la date et l’heure de reprise d’activité du système, les données qui ont été récupérées/perdues…

 Il précisera également la démarche que devront suivre les utilisateurs en cas de difficultés dans le fonctionnement des applicatifs redémarrés : précautions de redémarrage, personnes à contacter…

## Pour aller plus loin

Pour compléter le PRA du système d’information, l’établissement de santé pourra notamment intégrer des informations relatives :

 – À l’infrastructure technique de l’établissement de santé : cartographie de l’infrastructure technique, lieu géographique de l’infrastructure, description de la salle informatique, du centre d’hébergement… ;

 – Aux principes de sécurité qu’il aura définis pour garantir la continuité d’activité et le retour à la normale du système d’information en cas de panne : sécurité des serveurs, supervision et contrôle, protection logicielle, stockage…

### Infrastructure technique

**Présentation de l’architecture technique**

|  |
| --- |
| Cette section décrit les ressources techniques de l’établissement de santé. La cartographie technique du système d’information pourra ainsi être ici intégrée. Pourront également être précisées des informations relatives à la liste des serveurs exploités : serveur de données, d’application, serveurs disponibles par environnement…  |

**Sites géographiques**

Cette section présente la localisation géographique de l’infrastructure technique de l’établissement de santé, selon que celle-ci soit hébergée sur un site unique, ou réparti sur des lieux géographiques distincts.

Il convient donc de ne conserver ici que le paragraphe correspondant à la situation de l’établissement de santé, puis de le renseigner des informations indiquées.

**Hébergement**

* Votre établissement a confié l’hébergement de son système d’information à un tiers :

L’infrastructure technique du ***[nom de l’établissement de santé]*** est hébergée par ***[nom de la société en charge de l’hébergement de l’infrastructure technique de l’établissement].***

Elle est ***[localisée sur un seul site géographique/réparti (e) sur plusieurs sites comme suit :***

* ***Localisation géographie de la salle informatique ;***
* ***Localisation géographique du centre d’hébergement (le site de production et le site de secours).***
* Votre établissement héberge le système d’information :

L’établissement de santé héberge lui-même l’infrastructure technique. Celle-ci est ***[localisée sur un seul site géographique/réparti (e) sur plusieurs sites géographiques comme suit :***

* ***Localisation géographique de la salle ou des salles informatique.***

**Description des locaux**

Cette section présente les caractéristiques de sécurisation des locaux qui hébergent l’infrastructure technique de l’établissement de santé. Pour chaque local identifié, les informations suivantes sont notamment précisées :

 – La sécurisation de l’accès aux locaux ;

 – L’alimentation électrique ;

 – La climatisation ;

 – La sécurité en cas de dégâts des eaux ;

 – La sécurité incendie.

L’établissement de santé ajoutera ici toute information sur les caractéristiques de sécurisation des locaux hébergeant l’infrastructure technique qu’il juge pertinent d’intégrer au présent PRA.

De plus, il ajoutera en tant que de besoin les autres locaux qui n’hébergent pas l’infrastructure technique de l’établissement, mais qui pourraient avoir un impact sur le fonctionnement des équipements de l’infrastructure technique (ex : salle de l’auto commutateur).

Les caractéristiques générales de sécurisation de la salle informatique sont présentées ci-après.

* ***La sécurisation de l’accès à la salle informatique***

Les informations suivantes sur la sécurisation de l’accès à la salle informatique seront notamment indiquées :

 – La localisation de la salle informatique (site géographique, emplacement au sein de l’établissement…) ;

 – Le mode de sécurisation de l’accès à la salle informatique (porte blindée, digicode, alarme, caméra de surveillance, contrôle des mouvements…)

* ***L’alimentation électrique***

Les informations suivantes sur le système d’alimentation électrique seront notamment indiquées :

 – La présence d’onduleurs permettant d’assurer le fonctionnement du système et sa mise en sécurité ;

 – La présence de groupes électrogènes de secours en cas de coupures d’électricité prolongées ;

 – Les modalités de remontée d’alertes en cas d’incident électrique ;

 – Les procédures de tests mises en œuvre pour vérifier le bon fonctionnement du système ;

 – Le service (la personne) responsable de la maintenance du système d’alimentation électrique ;

 – Les dispositions du contrat de maintenance du système.

* ***La climatisation***

Les informations suivantes sur le système de climatisation seront notamment indiquées :

 – La puissance du système de climatisation ;

 – La température maintenue dans la salle informatique ;

 – Les modalités de remontée d’alertes en cas d’arrêt du système de climatisation ;

 – Les procédures de tests mises en œuvre pour vérifier le bon fonctionnement du système ;

 Le service (la personne) responsable de la maintenance du système de climatisation ;

 – Les dispositions du contrat de maintenance du système de climatisation.

* ***La sécurité en cas de dégâts des eaux***

Les informations suivantes sur la sécurité mise en place en cas de dégâts des eaux seront notamment indiquées :

 – Les modalités d’alerte en cas de présence d’eau (ex : système de détection, vase de rétention d’eau…) ;

 – L’équipement installé pour évacuer l’eau (ex. : pompes de refoulement…) ;

 – Les procédures de tests mises en œuvre pour vérifier le bon fonctionnement du système d’alerte et de l’équipement.

* ***La sécurité incendie***

Les informations suivantes sur le système de détection d’incendie seront notamment indiquées :

 – L’équipement mis en place pour détecter/éteindre un incendie ;

 – Les procédures de tests mises en œuvre pour vérifier le bon fonctionnement du système ;

 Le service (la personne) responsable de la maintenance du système de détection d’incendie ;

 – Les dispositions du contrat de maintenance du système de détection et d’extinction d’incendie.

* ***Réseau et transport de données***

Les informations suivantes sur le réseau de l’établissement de santé et les modalités de transport des données pourront notamment décrites :

 – L’architecture du réseau (topologie du réseau local [LAN], WAN, protocoles de communication, bande passante, etc.) ;

 – La description des services offerts par les opérateurs télécoms pour les échanges de l’établissement de santé avec l’extérieur (liaison spécifique/internet, bande passante garantie pour les échanges, engagements en cas de panne, etc.)

### Principes de sécurité

Cette section expose les principes de sécurité définis par l’établissement pour garantir la continuité d’activité et le retour à la normale du système d’information en cas de panne. Elle contient notamment les principes établis en matière de :

 – Sécurité des serveurs ;

 – Supervision et contrôles du système d’information ;

 – Protection des logiciels ;

 – Stockage.

L’établissement de santé pourra s’appuyer sur les termes des Contrats conclus avec les sociétés chargées de la maintenance du système d’information pour renseigner cette section.

Par ailleurs, l’établissement de santé ajoutera ici toute information sur les principes de sécurité qu’il juge pertinent d’intégrer au présent PRA. Néanmoins, les éléments détaillés dans cette partie ne doivent pas se substituer à une politique de sécurité des systèmes d’information qui doit être formalisée et éventuellement faire référence au PRA.

* ***Sécurité des serveurs***

Les informations suivantes sur la sécurité des serveurs seront notamment indiquées :

 – Le nombre et la description des serveurs (serveurs physiques/virtuels) ;

 – Le cas échéant, la description de la plateforme gérant les serveurs virtuels ;

 – La périodicité de réplication des serveurs du centre de production vers ceux du centre de secours ;

 – Les modalités de reprise de l’activité d’un serveur en cas de panne ;

 – La disponibilité des applications en cas de panne d’un serveur prévue par le Contrat conclu avec la société chargée de la maintenance du SI le cas échéant ;

– La procédure de bascule des serveurs et applications actifs du site de production vers le site de secours.

* ***Supervision et contrôle***

Les informations suivantes sur les procédures de supervision et de contrôle du système d’information de l’établissement seront notamment indiquées :

 – Les acteurs responsables de la surveillance du système (établissement, société de maintenance...) ;

 – La description du système d’alerte mis en place en cas de dysfonctionnements ;

 – Les modalités de remontées de ces alertes auprès des acteurs concernés ;

 – Les horaires d’astreintes du support de supervision et de contrôle.

* ***Protection logicielle***

Les informations suivantes sur les protections installées afin de protéger l’infrastructure technique de l’établissement seront notamment indiquées :

 – La protection des serveurs : mise à jour des OS, protections contre les logiciels malveillants… ;

 – La protection des postes de travail : mise à jour des OS, protections contre les logiciels malveillants… ;

 – La protection de la messagerie : logiciel antispam, vérification des emails entrants et sortants...

* ***Stockage***

Cette section présente les principes de stockage des serveurs et des documents bureautiques créés par les utilisateurs du système d’information de l’établissement de santé.

* ***Les environnements***

Cette section présente les environnements — de production, de test, de formation — dont dispose l’établissement de santé. Les informations suivantes seront notamment indiquées :

 – L’existence ou non d’environnements par application (production, test, formation) ;

 – Les règles d’accès à ces environnements (carte, codes d’accès…) ;

 – Les principes de test et de formation des utilisateurs à une nouvelle application sur ces environnements.

L’établissement de santé pourra ajouter ici toute information sur les environnements qu’il juge pertinent d’intégrer dans le présent PRA.