



PANNE ELECTRIQUE – REFLEXES

EN CAS DE PANNE ELECTRIQUE

Il faut identifier l'origine de la panne :

1. Interne : disjoncteur, réseau électrique interne, etc.
2. Externe : réseau du bâtiment, etc.
3. Fournisseur et/ou distributeur d'électricité
4. Action malveillante : débranchement, etc.
5. Intervention accidentelle sur l'alimentation

RISQUES

- ➔ **PERTE MOMENTANEE / DEFINITIVE DES DONNEES**
- ➔ **PERTURBATION / ARRET DE L'ACTIVITE**

GRAVE OU PAS ?

Le niveau de criticité de la panne électrique dépend :

- des services impactés (problème au niveau d'un seul serveur, de plusieurs, dans une même salle, réparti)
- de la durée d'interruption de l'activité
- de la nature des données impactées et la durée d'indisponibilité de ces données par rapport à la Durée Maximale d'Interruption Admissible (DMIA).

PREVENTION (MESURES A EVALUER SELON VOTRE CONTEXTE)

1. Renforcer la résilience de l'alimentation électrique :
 - S'équiper d'un groupe électrogène ou d'une seconde alimentation ondulée, indépendante, et mettre en place une alarme en cas de coupure sur l'alimentation principale
 - Tester régulièrement le dispositif en cas de coupure électrique (à raison d'au moins une fois par an)
 - Vérifier la conformité des installations et le bon dimensionnement des réseaux et équipements
2. En cas d'altération des systèmes et de la perte de données liées à une panne électrique, mettre en place une sauvegarde des environnements et des données afin de pouvoir restaurer le système
3. Disposer d'une organisation de gestion de crise et d'un plan de continuité informatique définissant les actions prioritaires en cas de panne électrique¹
4. Définir une procédure d'arrêt et une procédure de relance (en s'appuyant sur les procédures définies dans les dossiers d'exploitation)

ACTIONS A REALISER EN VUE DE LA REPRISE D'ACTIVITE

1. Vérifier le retour à la normale des services électriques
2. Vérifier que les cartes d'alimentation des machines sont toujours opérationnelles
3. Démarrer les services dans l'ordre défini dans la procédure de relance
4. Contrôler le retour à la normale des services / applications
5. Contrôler les éventuels problèmes d'intégrité (en cas de perte de données, fichiers corrompus ...)
6. Si les systèmes sont altérés ou les données perdues, restaurer les sauvegardes
7. En cas d'impacts critiques sur la prise en charge ou sur le fonctionnement de la structure (en particulier indisponibilité prolongée des SI), activer la cellule de crise et évaluer la nécessité de communiquer auprès des professionnels, des patients, de l'ARS et des directions du ministère

¹ http://esante.gouv.fr/sites/default/files/asset/document/pgssi-s_guide_pci_v0_3.pdf