

**LES BASES DE LA CYBERSECURITE**

Actions préventives à mettre en œuvre et conduite à tenir en cas de cyberattaque

### Service émetteur : DIS

### Rennes, le 2 août 2023



1. **- CONTEXTE**

Le numérique est devenu incontournable dans notre système de santé. Il permet le décloisonnement et une meilleure coordination des professionnels. Il favorise les innovations thérapeutiques et organisationnelles. Il replace l’individu au cœur des organisations de soin. Paradoxalement, les flux croissants et l’échange nécessaire d’informations sont autant de prises de risque pour la sécurisation des données et donc in fine pour la prise en charge des individus.

La menace est réelle comme en témoignent de récents évènements. Face à cela, il n’est plus possible de faire de la cybersécurité une variable d’ajustement des systèmes d’information en santé.

Les recommandations ci-dessous, concrètes, claires et simples vous permettront de mettre en place des mesures pour une protection globale de votre établissement mais également de savoir comment réagir en cas de cyberattaque.

1. **– 12 ACTIONS PRIORITAIRES A METTRE EN OEUVRE**

11 – Faire évaluer la couverture de sa police d’assurance au risque cyber

* Connaitre et faire évoluer son contrat

12 – Maitriser les risques numériques liés à vos relations avec des tiers

* Rédiger des contrats qui incluent des exigences précises pour lesquelles les tiers s’engagent
* Points de vigilance concernant les contrats
* Suivre et évaluer le respect des exigences de sécurité par les tiers

10 – Sensibiliser vos collaborateurs

* Connaitre les acteurs
* S’informer et sensibiliser

Pour en savoir plus : [Lettres d’information - Assistance aux victimes de cybermalveillance](https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/lettres-d-information)

9 – Maitriser le risque numérique lié au nomadisme des professionnels

* Sécuriser la mobilité numérique
* Avoir les bons réflexes durant les déplacements

Pour en savoir plus : [Bonnes pratiques à l’usage des professionnels en déplacement | Agence nationale de la sécurité des systèmes d'information](https://www.ssi.gouv.fr/guide/partir-en-mission-avec-son-telephone-sa-tablette-ou-son-ordinateur-portable/)

7 – Sécuriser sa messagerie

* Adopter les bons reflexes
* Configurer sa messagerie

Pour en savoir plus : [5 réflexes à avoir lors de la réception d’un courriel | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)](https://www.ssi.gouv.fr/entreprise/precautions-elementaires/5-reflexes-a-avoir-lors-de-la-reception-dun-courriel/)

8 – Séparez vos comptes et vos usages informatiques

* Connaitre les risques
* Créer et gérer des comptes utilisateurs
* Administrer son SI

Pour en savoir plus : [Recommandations relatives à l’administration sécurisée des systèmes d’information | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)](https://www.ssi.gouv.fr/guide/securiser-ladministration-des-systemes-dinformation/)

6 – Mettre en œuvre un pare-feu & règles de filtrage

* Activer son pare-feu local
* Installer un pare-feu physique

Pour en savoir plus : [guide\_preconisations-pare-feux-zone-exposee-internet\_anssi\_pa\_044\_v1.pdf](https://www.ssi.gouv.fr/uploads/2018/01/guide_preconisations-pare-feux-zone-exposee-internet_anssi_pa_044_v1.pdf)

4 – Utiliser un antivirus

* Déployer un antivirus sur tous les équipements

Pour en savoir plus : [Les antivirus - Assistance aux victimes de cybermalveillance](https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/antivirus)

1 – Réaliser l’inventaire complet de son système d’information

* Inventorier les équipements et services
* Inventorier les logiciels
* Inventorier les données et traitements
* Inventorier les accès
* Inventorier les interconnexions avec l’extérieur
* Mettre à jour régulièrement les différents inventaires

Pour en savoir plus : [guide-cartographie-systeme-information-anssi-pa-046.pdf](https://www.ssi.gouv.fr/uploads/2018/11/guide-cartographie-systeme-information-anssi-pa-046.pdf)

2 – Réaliser des sauvegardes régulières

* Identifier les sauvegardes à réaliser
* Déterminer le rythme des sauvegardes
* Choisir le ou les supports à privilégier pour la sauvegarde
* Evaluer la pertinence du chiffrement des données
* Respecter le cadre juridique
* Mettre à jour régulièrement les différents inventaires

Pour en savoir plus : [Pourquoi et comment bien gérer ses sauvegardes ? - Assistance aux victimes de cybermalveillance](https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes#:~:text=La%20plupart%20des%20solutions%20de,r%C3%A9alisez%20des%20sauvegardes%20manuelles%20r%C3%A9guli%C3%A8rement.)

5 – Implémenter une politique d’usage de mots de passe robustes

* Choisir des mots de passe robustes
* Définir une bonne politique de mot de passe
* L’authentification unifiée

Pour en savoir plus : [Pourquoi et comment bien gérer ses mots de passe ? - Assistance aux victimes de cybermalveillance](https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe)

3 – Appliquer régulièrement les mises à jour

* Utiliser des solutions matérielles et logicielles maintenues
* Activer la mise a jour automatique des logiciels et matériels

Pour en savoir plus : [Pourquoi et comment bien gérer ses mises à jour ? - Assistance aux victimes de cybermalveillance](https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mises-a-jour)

1. **– COMMENT REAGIR EN CAS DE CYBERATTAQUE**

**1 – Se préparer à l’incident**

🡪Vous avez tout avantage à identifier préalablement des prestataires spécialisés dans la réponse aux incidents de sécurité.

Le CERT Santé apporte un appui en cas d’incident de sécurité des systèmes d’information : il assure une mission de prévention et d’alerte face aux menaces de cybersécurité et partage différentes recommandations pour minimiser les effets en cas de cyberattaque. En parallèle, il est également possible de contacter votre ARS ou votre GRADeS : leurs experts peuvent vous orienter vers une assistance appropriée.

* CERT Santé : Le CERT Santé assure le traitement des signalements des incidents de sécurité les jours ouvrés de 9h à 18h et, en urgence,**24h/24 et 7j/7**par téléphone au **+33 (0)9 72 43 91 25 -** [**cyberveille@esante.gouv.fr**](mailto:cyberveille@esante.gouv.fr)
* ARS Bretagne : [ars-bretagne-dis@ars.sante.fr](mailto:ars-bretagne-dis@ars.sante.fr)
* GCS e-Santé Bretagne : [ssi@esante-bretagne.fr](mailto:ssi@esante-bretagne.fr)
* Prestataires de réponse aux incidents de sécurité : [Prestataires de réponse aux incidents de sécurité PRIS | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)](https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-reponse-aux-incidents-de-securite-pris/)

**2 – En cas d’incident avéré**

1 - Le premier réflexe à avoir en cas d’incident concernant un système d’information est de **déconnecter son équipement ou son système d’information d’entreprise d’Internet.**

Pour un équipement individuel, cela peut se traduire par le retrait de la prise ou la désactivation des services WiFi. Pour un SI d’établissement, l’action peut être menée sur l’équipement réseau ou le pare-feu. Cela évitera une fuite éventuelle de données.

**2 - N’éteignez pas, ni ne modifiez, les ordinateurs et matériels affectés par l’attaque : ils seront utiles aux enquêteurs.**

**3 - En cas de rançongiciel, ne payez jamais la rançon demandée :** des solutions de déchiffrement existent et vous serez assistés par des gardiens de la paix.

🡪Vos sauvegardes vous permettront de retrouver une activité normale.

4 - Il est recommandé d’**ouvrir une main courante** pour tracer les actions et événements liés à l’incident, (l’heure et la date de l’action ou de l’événement, le nom de la personne à l’origine de cette action ou ayant informée sur l’événement, la description de l’action ou de l’événement). La tenue d’une main courante régulièrement alimentée tout au long de l’incident va considérablement faciliter l’intervention du prestataire et la résolution du problème.

5 - **Pour une structure, il convient de préparer un dispositif d’information relatif à l’incident.** Ce dispositif doit être proposé par le référent communication (en lien avec les experts techniques) et porté par la direction. La charte informatique peut également informer les collaborateurs de la bonne attitude à avoir en cas d’incident avéré. A noter sur l’article 34 du règlement RGDP :

***Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé*** *pour les droits et libertés d'une personne physique, le* ***responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais****.*

*La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d).*

*La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie:*

*a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement;*

*b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser;*

*c)****elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace***.

**Signalement des incidents « significatifs ou graves » de sécurité informatique :**

Le décret no 2022-715 du 27 avril 2022 relatif aux conditions et aux modalités de mise en œuvre du signalement des incidents significatifs ou graves de sécurité des systèmes d’information prévoit pour les structures de santé **une obligation de signalement à l’Agence du Numérique en Santé (ANS) des incidents « significatifs ou graves » de sécurité informatique.**

6 - La déclaration doit être réalisée via le Portail de signalement des événements sanitaires indésirables : <https://signalement.social-sante.gouv.fr/>

7 - En parallèle, il vous est également possible d’informer par mail votre ARS : [ars-bretagne-dis@ars.sante.fr](mailto:ars-bretagne-dis@ars.sante.fr)

**8 - Il est également essentiel de porter plainte auprès de votre commissariat de police ou de gendarmerie.**

9 - Si l’incident implique des données personnelles et présente un risque pour les droits et libertés des personnes, vous devez également informer la CNIL dans les 72h : [Notifier une violation de données personnelles | CNIL](https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles)

10 - Pour les établissements qui sont OSE (Opérateurs de Services Essentiels), ils doivent également déclarer l’incident auprès de l’ANSSI : [En cas d’incident | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)](https://www.ssi.gouv.fr/en-cas-dincident/)

1. **– POUR ALLER PLUS LOIN**

[ANS\_GUIDECYBER\_PHASE 1-EXE -V2.pdf (esante.gouv.fr)](https://esante.gouv.fr/sites/default/files/media_entity/documents/ANS_GUIDECYBER_PHASE%201-EXE%20-V2.pdf)

[Attaques par rançongiciels, tous concernés – Comment les anticiper et réagir en cas d’incident ? | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)](https://www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/)