

# **CAHIER DES CLAUSES TECHNIQUES PARTICULIERES**

**GROUPEMENT DE COMMANDE DE SERVICES D'ASSURANCE  
POUR 2 ETABLISSEMENTS DE SANTE**

**GROUPEMENT HOSPITALIER DE TERRITOIRE NORD YONNE**

Etablissement support :

**CENTRE HOSPITALIER  
1 AVENUE PIERRE DE COUBERTIN - BP 808  
89108 SENS CEDEX**

Objet du marché :

**LOT 6 : PRESTATIONS DE SERVICES D'ASSURANCES  
ASSURANCE CYBER-RISQUES**

Le présent document comporte 15 pages, numérotées de 1 à 15.

## SOMMAIRE

<b>1- PREAMBULE .....</b>	<b>4</b>
1.1. SOUSCRIPTEUR : .....	ERREUR ! SIGNET NON DEFINI.
1.2. ASSURE (s).....	4
1.3. ACTIVITES .....	4
<b>2- DEFINITIONS CONTRACTUELLES .....</b>	<b>5</b>
2.1. ACTE DE MALVEILLANCE INFORMATIQUE : .....	5
2.2. INTRUSION RESEAU : .....	5
2.3. LOGICIEL MALVEILLANT : .....	5
2.4. HAMEÇONNAGE (PHISHING) : .....	5
2.5. CRYPTOLOCKER (RANSOMWARE) : .....	5
2.6. DENI DE SERVICE : .....	5
2.7. INTERRUPTION DE SERVICE MALVEILLANTE : .....	6
2.8. ERREUR HUMAINE : .....	6
2.9. EFFETS DU COURANT : .....	6
2.10. ATTEINTE A LA PROTECTION DES DONNEES PERSONNELLES* : .....	6
2.11. CYBER-ESPIONNAGE ECONOMIQUE OU INDUSTRIEL : .....	6
2.12. CYBER-EXTORSION DE FONDS : .....	6
2.13. CYBER DETOURNEMENT DE FONDS : .....	7
2.14. ATTEINTE MEDIATIQUE : .....	7
2.15. FRAUDE TELEPHONIQUE : .....	7
2.16. EXTORSION : .....	7
2.17. PENALITES REGLEMENTAIRES : .....	7
2.18. PERTE D'EXPLOITATION : .....	7
2.19. FRAIS DE NOTIFICATION : .....	8
2.20. FRAIS SUPPLEMENTAIRES D'EXPLOITATION : .....	8
2.21. FRAIS DE DEFENSE ET DE JUSTICE : .....	8
2.22. DOMMAGES ET INTERETS : .....	8
<b>3- EVENEMENTS ASSURES .....</b>	<b>9</b>
3.1. ATTEINTES AUX INFORMATIONS .....	9
3.2. ATTEINTE A LA PROTECTION DES DONNEES PERSONNELLES .....	9
3.3. ESPIONNAGE ECONOMIQUE .....	9
3.4. ATTEINTE MEDIATIQUE .....	9
3.5. DETOURNEMENT DE FONDS ET TENTATIVE D'EXTORSION DE FONDS .....	10

<b>3.6.</b>	<b>FRAUDE TELEPHONIQUE</b>	<b>10</b>
<b>3.7.</b>	<b>ATTAQUE PAR DENI DE SERVICE</b>	<b>10</b>
<b>3.8.</b>	<b>COMMUNICATION ET GESTION DE CRISE</b>	<b>10</b>
<b>3.9.</b>	<b>PERTE D'EXPLOITATION :</b>	<b>10</b>
<b>3.10.</b>	<b>PROTECTION JURIDIQUE ET FRAIS DE JUSTICE</b>	<b>10</b>
3.10.1	<i>Frais de défense :</i>	10
3.10.2	<i>Dommages et intérêts</i>	10
3.10.3	<i>Enquêtes et sanctions administratives</i>	11
<b>3.11.</b>	<b>FRAIS DE NOTIFICATION</b>	<b>11</b>
<b>3.12.</b>	<b>EXCLUSIONS</b>	<b>11</b>
<b>4-</b>	<b>DISPOSITIONS PARTICULIERES</b>	<b>12</b>
<b>4.1.</b>	<b>TERRITORIALITE – SITUATION DES RISQUES</b>	<b>12</b>
<b>4.2.</b>	<b>GARANTIE DANS LE TEMPS</b>	<b>12</b>
4.2.1	<i>Conditions de garantie en cours de validité du contrat et garantie subséquentes.</i>	12
<b>4.3.</b>	<b>CONFIDENTIALITE</b>	<b>12</b>
<b>4.4.</b>	<b>- LOI APPLICABLE ET TRIBUNAUX COMPETENTS</b>	<b>12</b>
<b>4.5.</b>	<b>MODIFICATION DU RISQUE</b>	<b>13</b>
4.5.1	<i>Acquisition et/ou création de nouveaux assure</i>	13
4.5.2	<i>Cession</i>	13
4.5.3	<i>Fusion absorption du souscripteur</i>	13
<b>5-</b>	<b>MONTANT DES GARANTIES ET DES FRANCHISES</b>	<b>14</b>
<b>6-</b>	<b>DOCUMENTS ANNEXES</b>	<b>15</b>

## **1- PREAMBULE**

Le présent marché a pour objet d'assurer l'établissement contre les risques liés à la cybercriminalité et notamment l'atteinte aux systèmes informatiques et/ou l'intégrité de leurs données intrusion, site internet indisponible, absence de sauvegarde, faille de sécurité, vol des données, logiciels espions, défaut de mise à jour de logiciels de sécurité, erreur humaine, extorsion de fond et demande de rançon.

Les garanties sont étendues aux données appartenant à des tiers et hébergées par l'Assuré.

L'Assureur déclare avoir eu la connaissance nécessaire à une juste appréciation des risques et ne pourra se prévaloir d'une absence de déclaration.

### 1.1. Assuré (s)

01\_ CENTRE HOSPITALIER DE SENS  
02\_ CENTRE HOSPITALIER DE JOIGNY

### 1.2. Activités

Etablissement public de santé.

## **2- DEFINITIONS CONTRACTUELLES**

### **2.1. ACTE DE MALVEILLANCE INFORMATIQUE :**

C'est le fait d'accéder ou de se maintenir frauduleusement dans un système informatique, ou le fait de supprimer, d'introduire ou de modifier frauduleusement des données dans un système informatique, ou encore le fait d'entraver, d'altérer ou de fausser frauduleusement le fonctionnement d'un système informatique (articles 323.1 à 323.7 du Code pénal). Font partie de la malveillance informatique l'attaque par déni de service, ainsi que toute infection informatique de type virus, cheval de Troie, bombe logique... introduites clandestinement ou accidentellement dans le système informatique.

### **2.2. INTRUSION RESEAU :**

L'intrusion réseau est constituée par l'un des événements suivants :

- L'accès et/ou l'utilisation non autorisés, réels ou supposés, d'un système informatique détenu ou contrôlé par l'assuré ou dont l'assuré est responsable.
- L'accès non autorisé, réel ou supposé, au système informatique en cause entraînant une atteinte aux données ou une atteinte médiatique.
- L'infection dudit système informatique par un logiciel malveillant ou la transmission d'un tel logiciel malveillant audit système informatique ou depuis celui-ci.
- Une attaque par déni de service.
- Des attaques informatiques de type « dévoiement » (pharming), hameçonnage (phishing).

Une série d'intrusions réseaux continues ou des intrusions liées, répétées ou semblables sont considérées comme un seul et unique fait dommageable, réputé avoir eu lieu au moment de la première intrusion.

### **2.3. LOGICIEL MALVEILLANT :**

Tout code informatique non autorisé ou de nature à créer des altérations ou des nuisances et qui est conçu pour pénétrer un système informatique et pour se propager d'un système informatique à un autre.

### **2.4. HAMEÇONNAGE (PHISHING) :**

L'hameçonnage est un type de cyber attaque dont l'objet est d'imiter la charte graphique du souscripteur dans le but de récupérer des informations importantes par le biais de la victime.

### **2.5. CRYPTOLOCKER (RANSOMWARE) :**

Le cryptolocker est un type de cyber attaque qui consiste à crypter les données de la victime à travers l'utilisation d'un logiciel malveillant afin de pouvoir demander une rançon à la victime.

### **2.6. DENI DE SERVICE :**

Attaque délibérée de hackers (pirates informatiques) à l'encontre d'un site internet, par la transmission volontaire d'un volume excessif de données, provoquant l'indisponibilité du site

internet du fait de sa saturation de capacité. L'attaque par déni de service est un cas particulier d'Acte de malveillance informatique.

## **2.7. INTERRUPTION DE SERVICE MALVEILLANTE :**

Toute coupure électrique ou toute interruption dans les moyens de télécommunication affectant l'installation de l'Assuré, ou les réseaux le reliant aux fournisseurs du fait d'un acte malveillant.

## **2.8. ERREUR HUMAINE :**

Erreur ayant pour origine une maladresse, une négligence, une erreur de manipulation, de paramétrage, une entrée de commande erronée, un lancement de programme inadéquat, et ayant pour effet la perte ou l'altération des données ou informations assurées.

## **2.9. EFFETS DU COURANT :**

Effets du courant, de phénomènes électriques, d'un champ magnétique conduisant à la perte ou l'altération des données informatiques de l'Assuré (exemple : décharge électrostatique, effets de la foudre, perturbation électromagnétique, surtension, sous-tension, panne de courant, disjonction ou coupure brutale du courant...).

## **2.10. ATTEINTE A LA PROTECTION DES DONNEES PERSONNELLES\* :**

Non-respect avéré de la Règlementation sur la protection des données personnelles. Ce non-respect doit avoir été commis involontairement par l'Assuré ou par les prestataires, fournisseurs ou sous-traitants tiers auxquels il a recouru pour le transfert de données et traitements, ou l'hébergement de son site internet, et doit faire suite à la divulgation non autorisée (au sens de la Règlementation précitée) de Données personnelles de ses clients.

**Donnée personnelle\***: Conformément à la loi « Informatique et Libertés » du 6 janvier 1978, [Modifié par LOI n°2018-493 du 20 juin 2018](#) constitue une donnée personnelle ou à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

## **2.11. CYBER-ESPIONNAGE ECONOMIQUE OU INDUSTRIEL :**

Introduction frauduleuse dans le Système informatique de l'Assuré dans le but d'y dérober, ou de copier, des données ou informations sensibles de l'entreprise afin d'être exploitées ou revendues à des tiers. L'acte malveillant peut avoir été perpétré par un tiers, avec ou sans la complicité d'un préposé, ou par un préposé.

## **2.12. CYBER-EXTORSION DE FONDS :**

Tentative d'un tiers d'extorquer une somme d'argent (rançon) après avoir commis un acte de malveillance sur le Système informatique de l'Assuré.

**2.13. CYBER DETOURNEMENT DE FONDS :**

Introduction frauduleuse dans le Système informatique de l'Assuré dans le but de dérober, des fonds ou valeurs. L'acte de détournement peut avoir été perpétré par un tiers, avec ou sans la complicité d'un préposé, ou par un préposé.

**2.14. ATTEINTE MEDIATIQUE :**

Tous dommages subis par un tiers ou l'assuré, directement ou indirectement liés à une divulgation ou diffusion illégale d'informations via un média détenu ou contrôlé par l'assuré ou concernant des informations dont l'assuré assume la responsabilité. La divulgation ou la diffusion peut résulter ou non d'une atteinte aux données ou d'une intrusion réseau.

Ceci inclut notamment les dommages causés par :

- ✓ Une diffamation, y compris les calomnies et déclarations mensongères ;
- ✓ Une atteinte à la protection de la vie privée de cette personne ;
- ✓ Une atteinte aux droits à l'image de cette personne, y compris toute utilisation incorrecte ou impropre ;
- ✓ Toute juxtaposition ou tout lien avec le nom, la personnalité, la voix ou la ressemblance de cette personne ;
- ✓ Une atteinte aux droits de propriété intellectuelle d'un tiers.

**2.15. FRAUDE TELEPHONIQUE :**

Toute introduction frauduleuse des systèmes de téléphonie de l'assuré entraînant une surfacturation téléphonique lorsqu'elle répercutée sur les factures téléphoniques délivrées par un opérateur.

**2.16. EXTORSION :**

Infraction, prévue à l'article 312-1 du Code Pénal français ou son équivalent dans toute législation étrangère applicable, dont est victime un assuré de la part d'un tiers ayant effectivement réalisé, ou menaçant de façon crédible, de réaliser une intrusion réseau, une atteinte aux données ou une atteinte médiatique.

**2.17. PENALITES REGLEMENTAIRES :**

Les amendes et pénalités civiles, dès lors qu'elles sont légalement assurables, émises par une autorité administrative, réglementaire ou gouvernementale et consécutives à une enquête menée par ces autorités à la suite d'une atteinte aux données.

**2.18. PERTE D'EXPLOITATION :**

La somme des montants que représentent la diminution du résultat net avant impôt et des frais opérationnels subis par l'assuré, au cours de la période de remise en état des systèmes, à la suite de l'impossibilité effective, provoquée ou imposée par une intrusion réseau, d'utiliser un système

EPS BARTHELEMY DURAND / MARCHE PUBLIC DE SERVICES D'ASSURANCES

CCTP LOT 5 - ASSURANCE CYBER-RISQUES

informatique détenu ou contrôlé par l'assuré ou dont il est responsable.

**2.19. FRAIS DE NOTIFICATION :**

Frais engagés rendus nécessaires pour l'identification des personnes physiques et des autorités auxquelles la violation de données personnelles devra être notifiée.

**2.20. FRAIS SUPPLEMENTAIRES D'EXPLOITATION :**

Frais engagés pour la mise en œuvre de mesures correctives permettant d'éviter, de limiter et de reprendre le plus rapidement possible les activités professionnelles.

**2.21. FRAIS DE DEFENSE ET DE JUSTICE :**

Frais de justice et d'honoraires d'avocat engagés à la suite d'un sinistre garantis et rendus nécessaires par une réclamation ou une obligation réglementaire.

**2.22. DOMMAGES ET INTERETS :**

Indemnités mis à la charge de l'assuré dans le cadre d'une décision de justice ou arbitrale.



### **3- EVENEMENTS ASSURES**

#### **3.1. ATTEINTES AUX INFORMATIONS**

Sont garantis les frais et pertes résultant d'une Atteinte aux informations et ayant pour origine :

- Un acte de malveillance informatique (dont virus et déni de service)
- Une interruption de service suite à acte de malveillance informatique sur l'installation du fournisseur d'électricité ou de télécommunication

En complément des événements garantis précités, sont garantis les frais ci-après définis résultant d'une Atteinte aux informations non consécutive à un dommage matériel et ayant pour origine :

- Une erreur humaine commise par imprudence ou négligence
- Une interruption de service suite à erreur humaine sur l'installation du fournisseur d'électricité ou de télécommunication
- Les effets du courant

#### **3.2. ATTEINTE A LA PROTECTION DES DONNEES PERSONNELLES**

Sont garantis les frais et pertes ci-après définis résultant d'une Atteinte à la protection des données personnelles c'est à dire la perte, l'altération, la divulgation ou l'accès non autorisé à des données personnelles et ayant pour origine :

- Un acte de malveillance informatique
- Une erreur humaine commise par imprudence ou négligence.

#### **3.3. ESPIONNAGE ECONOMIQUE**

Sont garantis les frais et pertes résultant l'introduction frauduleuse dans le Système informatique de l'Assuré dans le but d'y dérober, ou de copier, des données ou informations sensibles de l'entreprise afin d'être exploitées ou revendu. La malveillance pourra avoir été perpétré par un tiers, avec ou sans la complicité d'un préposé, ou par un préposé.

#### **3.4. ATTEINTE MEDIATIQUE**

Sont garantis les frais et pertes subis par un tiers ou l'assuré, directement ou indirectement liés à une divulgation ou diffusion illégale d'informations via un média détenu ou contrôlé par l'assuré ou concernant des informations dont l'assuré assume la responsabilité. La divulgation ou la diffusion peut résulter ou non d'une atteinte aux données ou d'une intrusion réseau.

Sont ainsi garantis les dommages causés par :

- ✓ Une diffamation, y compris les calomnies et déclarations mensongères.
- ✓ Une atteinte à la protection de la vie privée.

- ✓ Une atteinte aux droits à l'image.
- ✓ Une atteinte aux droits de propriété intellectuelle.

### **3.5. DETOURNEMENT DE FONDS ET TENTATIVE D'EXTORSION DE FONDS**

Seront garantis les frais et pertes consécutives à une introduction frauduleuse dans le Système informatique de l'Assuré dans le but de dérober, des fonds, y compris une demande de rançon. Le détournement peut avoir été perpétré par un tiers, avec ou sans la complicité d'un préposé, ou par un préposé.

### **3.6. FRAUDE TELEPHONIQUE**

Seront garantis les frais et pertes consécutives à une surfacturation téléphonique lorsqu'elle est répercutée sur les factures téléphoniques délivrées par un opérateur.

### **3.7. ATTAQUE PAR DENI DE SERVICE**

Le déni de service consiste à envoyer un très grand nombre de requêtes dans le but d'empêcher une entreprise de fournir un service du fait de la saturation du système informatique.

### **3.8. COMMUNICATION ET GESTION DE CRISE**

Seront garanties les frais et horaires de spécialistes en communication de crise rendus nécessaires pour la gestion de la communication externe et interne à l'assuré en vue de limiter l'impact d'un sinistre sur la réputation.

### **3.9. PERTE D'EXPLOITATION :**

Seront garantis les pertes de marge brute d'exploitation subie directement subie par l'interruption des activités professionnelles et consécutives à la survenance d'un sinistre garanti.

### **3.10. PROTECTION JURIDIQUE ET FRAIS DE JUSTICE**

#### **3.10.1 Frais de défense :**

Seront garantis les frais d'avocat engagés par l'assuré. Cette prise en charge interviendra à l'issue du règlement amiable, arbitral, administratif ou judiciaire du sinistre.

#### **3.10.2 Dommages et intérêts**

Seront garantis les dommages et intérêts auxquels l'assuré serait condamné à l'issue d'une décision arbitrale, administrative ou judiciaire.

### 3.10.3 Enquêtes et sanctions administratives

Seront garantis les dépenses engagées en cas d'enquête ou action diligentée à l'encontre de l'assuré par une autorité administrative ou gouvernementale compétente au titre de la violation de données personnelles concernée, notamment la Commission Nationale Informatique et Libertés.

### 3.11. **FRAIS DE NOTIFICATION**

Seront garantis les frais engagés permettant de procéder :

- ✓ A l'identification de la nature et de la portée de vos obligations légales ou réglementaires de notification.
- ✓ A l'identification des personnes physiques et des autorités nationales auxquelles la violation de données personnelles constatée devra être notifiée.
- ✓ A la notification de la violation de données personnelles constatée aux personnes physiques concernées et aux autorités administratives ou gouvernementales compétentes conformément à vos obligations légales ou réglementaires.

### 3.12. **EXCLUSIONS**

Les exclusions contenues dans les offres figurent au nombre des critères de sélection.

Par conséquent, il appartient aux assureurs de respecter l'esprit et l'amplitude des définitions de garanties en limitant au minimum les exclusions concernant l'application des garanties. Elles devront impérativement être indiquées en réserves dans le cadre prévu à cet effet dans l'annexe de prix.

## **4- DISPOSITIONS PARTICULIERES**

### **4.1. TERRITORIALITE – SITUATION DES RISQUES**

L'ensemble des garanties s'exercent pour les Systèmes informatiques dont l'activité se situe dans l'ensemble des pays de l'Union Européenne, en Suisse, Andorre, Monaco et Grande Bretagne.

### **4.2. GARANTIE DANS LE TEMPS**

Le présent article reproduit aux paragraphes 3.4.1, 3.4.2, 3.4.3, 3.4.4 ci-après les dispositions du 4° alinéa de l'article L 124-5 du Code des assurances conformément à l'obligation faite à l'assureur.

#### **4.2.1 Conditions de garantie en cours de validité du contrat et garantie subséquentes.**

La garantie du présent contrat est déclenchée par la réclamation et couvre l'assuré contre les conséquences pécuniaires des sinistres, dès lors que le fait dommageable est antérieur à la date de résiliation ou d'expiration de la garantie, et que la première réclamation lui est adressée ou est adressée à l'assureur entre la prise d'effet initiale de la garantie et l'expiration d'un délai subséquent de cinq (5) ans à compter de sa date de résiliation ou d'expiration quelle que soit la date des autres éléments constitutifs des sinistres.

### **4.3. CONFIDENTIALITE**

L'assureur traitera de façon confidentielle les informations fournies par le souscripteur dans le cadre de la police et de tout sinistre y afférent. L'assureur ne communiquera à aucun tiers ces informations sans avoir préalablement obtenu l'accord du souscripteur. Toutefois l'assureur pourra être autorisé après accord de l'assuré à divulguer les informations confidentielles :

- ✓ Aux experts sinistres impliqués dans la gestion de la police, aux membres de son personnel, à ses représentants, réassureurs et conseillers professionnels, ainsi qu'à ceux de son groupe de sociétés.
- ✓ Que la loi, la réglementation applicable ou une décision de justice obligerait à communiquer.
- ✓ À tout tribunal, organisme de médiation ou d'arbitrage auquel serait référé toute affaire relative à la police ou à sa réassurance.

### **4.4. - LOI APPLICABLE ET TRIBUNAUX COMPETENTS**

Le présent contrat est soumis au droit français.

Tout litige relatif à l'application du présent contrat sera obligatoirement du ressort exclusif des tribunaux français.

#### **4.5. MODIFICATION DU RISQUE**

##### **4.5.1 Acquisition et/ou création de nouveaux assure**

La garantie est automatiquement étendue à toute personne morale qui, pendant la période de garantie acquière la qualité assurée.

##### **4.5.2 Cession**

Dans l'hypothèse où une personne morale cesse d'avoir la qualité d'assuré en cours de période de garantie, la garantie lui reste acquise pour les réclamations portant sur des fautes commises antérieurement à la date de cession pendant la période de validité du contrat et au-delà, pendant la garantie subséquente.

##### **4.5.3 Fusion absorption du souscripteur**

Le présent contrat est automatiquement résilié à l'issue de la période de garantie au cours de laquelle est intervenue une fusion absorption entraînant la disparition du souscripteur au bénéfice d'une personne morale autre qu'un assuré, sauf demande expresse du souscripteur.

#### **4.6. COTISATIONS**

Les cotisations sont forfaitaires par établissement.

## 5- MONTANT DES GARANTIES ET DES FRANCHISES

Montant des garanties	1.000.000 € par sinistre et par an
Dont	
Enquêtes administratives	500.000 €
Amendes administratives	500.000 €
Frais de communication de crise	500.000 €
Frais de de défense	500.000 €
Frais de notification	500.000 €
Pertes d'exploitation	1.000.000 €
Fraude téléphonique	150.000 €

Les garanties sont accordées au premier risque avec dérogation à la règle proportionnelle, par sinistre, c'est-à-dire par événement et par site, sans limitations annuelles.

Elles sont automatiquement reconstituées après la survenance d'un sinistre, sans perception de primes complémentaires.

**Franchise par événement : 10 000 €**

## 6- DOCUMENTS ANNEXES

- **Document** : Questionnaire cyber-risques
- **Document** : Fichier information activité
- **Ce risque n'a jamais été assuré**
- Annexe de prix à joindre **obligatoirement** à l'acte d'engagement