

CONDITIONS GÉNÉRALES DE RÉPONSE À INCIDENT

applicables à toute entité qui sollicite une Assistance de

l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

pour le traitement d'un incident de sécurité sur ses systèmes d'information

L'ANSSI est un service à compétence nationale rattaché au secrétaire général de la défense et de la sécurité nationale, créé par le décret n° 2009-834 du 7 juillet 2009. Elle est l'autorité nationale de défense et de sécurité des systèmes d'information. À ce titre, l'ANSSI mène des recherches de compromissions ou d'incidents de sécurité et peut apporter son concours pour y répondre.

L'ANSSI est susceptible de demander son concours à d'autres services de l'Etat notamment les services du Ministère des Armées dans le cadre de l'instruction interministérielle du 18 janvier 1984, modifiée, relative à la participation des armées à des missions relevant d'autres départements ministériels.

DÉFINITIONS

Les termes précédés d'une majuscule ont le sens que les Parties entendent leur donner. En l'absence de majuscule, les termes reprennent leur sens usuel. Les Parties conviennent des définitions suivantes :

Assistance : ensemble de services fournis par l'ANSSI afin d'apporter son concours pour traiter un incident de sécurité. À cette fin, l'ANSSI peut procéder notamment à :

- la réalisation d'activités d'Expertise ;
- des opérations de Remédiation sur les Systèmes d'information et équipements compromis ;
- la proposition d'éléments de communication de crise.

Bénéficiaire : organisme qui reçoit une Assistance en tout ou partie dans sa gestion d'un incident de cybersécurité.

Conditions générales de Réponse à Incident : le présent document.

Évènement de sécurité : occurrence identifiée de l'état d'un système, d'un service ou d'un réseau indiquant une faille possible dans la politique de sécurité des systèmes d'information ou un échec des mesures de sécurité ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité des systèmes d'information.

Incident de sécurité : un incident de sécurité est indiqué par un ou plusieurs Évènement(s) de sécurité indésirable(s) ou inattendu(s) présentant une probabilité forte de

compromettre les opérations liées à l'activité de l'organisme et/ou de menacer la sécurité des systèmes d'information.

Marqueur/Signature : élément technique permettant de caractériser et de signaler un Évènement de sécurité.

Expertise : service technique fourni par l'ANSSI ou l'un de ses Partenaires afin de définir l'état de compromission de ces systèmes d'information et de proposer les contre-mesures nécessaires et pouvant comprendre

- la conduite d'entretiens avec les équipes du Bénéficiaire et l'analyse de documents fournis par le Bénéficiaire pour la prise en compte du contexte ;
- la collecte d'éléments techniques issus des Systèmes d'information du Bénéficiaire à des fins d'investigation ou issus d'audit à des fins de contextualisation ;
- la recherche de tout type de compromission également à travers de la supervision de circonstance¹ ;
- l'analyse des vulnérabilités des systèmes d'information du Bénéficiaire ;
- l'analyse de la nature des Incidents de sécurité et du fonctionnement des attaques.

Partenaire : l'un des prestataires de réponse à incident intervenant pour le compte de l'ANSSI ou un autre service de l'Etat qui apporte son concours à l'ANSSI dans la réponse à incident.

Partie(s) : désigne le Bénéficiaire ou l'ANSSI ou le Partenaire. Au pluriel, désigne conjointement l'ANSSI et le Bénéficiaire.

Relevés techniques : l'ensemble des traces techniques (images disques, images mémoire, journaux d'Évènements, alertes, traces système, réseau et applicatives) obtenues lors de l'Expertise.

¹ Supervision de circonstance : définie dans le [référentiel de Prestataires de Réponse à Incident de Sécurité](#) (PRIS) publié par l'ANSSI.

Remédiation : préconisation de mesures visant à limiter une compromission, enrayer l'activité d'un attaquant et durcir la sécurité du système d'information cible de la prestation.

Système d'information : ensemble organisé de ressources (matériel, logiciels, personnel, données et procédures) permettant de traiter et de diffuser de l'information.

ARTICLE 1 OBJET

Les présentes Conditions générales de Réponse à Incident ont pour objet d'encadrer l'Assistance pour le traitement d'un ou plusieurs Incidents de sécurité et de déterminer les conditions pratiques et juridiques de réalisation de celui-ci.

Toute Assistance au profit du Bénéficiaire entraîne l'acceptation sans réserve des Conditions générales de Réponse à Incident par le Bénéficiaire.

ARTICLE 2 DURÉE — RÉSILIATION

Les Conditions générales de Réponse à Incident s'appliquent au Bénéficiaire dès lors qu'il sollicite une Assistance de l'ANSSI pour résoudre un Incident de sécurité. Les Conditions générales de Réponse à Incident sont dès lors applicables pour la durée de l'Assistance, sauf résiliation par l'une ou l'autre des Parties.

L'ANSSI n'est pas tenue de donner suite à une demande d'assistance du Bénéficiaire. L'opportunité d'intervenir reste soumise à la libre appréciation de l'ANSSI. Elle n'est pas tenue de justifier son refus d'intervenir.

Chacune des Parties peut résilier unilatéralement les Conditions générales de Réponse à Incident moyennant le respect d'un délai de préavis de quinze (15) jours calendaires.

En cas de nécessité de service, l'ANSSI se réserve le droit de suspendre toute Assistance de manière unilatérale et sans délai. Dans ce cas, l'ANSSI s'engage à en informer le Bénéficiaire dans les meilleurs délais.

ARTICLE 3 OBLIGATIONS GÉNÉRALES DES PARTIES

3.1 Obligations de l'ANSSI

L'ANSSI s'engage à solliciter l'accord préalable du Bénéficiaire avant de faire appel à l'un de ses Partenaires.

L'ANSSI, le cas échéant le Partenaire, s'engagent pendant toute la durée de l'Assistance :

- à ne pas volontairement prendre connaissance d'informations relevant du secret de la défense nationale se trouvant dans les Systèmes d'Information du Bénéficiaire, à l'exception des données du Bénéficiaire nécessaires à la Réponse à Incident ;

- à collecter et analyser ou faire collecter et faire analyser les données ou les matériels du Bénéficiaire, suspectés de compromission et jugés utiles pour l'investigation, sur un réseau sécurisé et adapté au niveau de sensibilité des données et matériels ;
- à avertir ou faire avertir sans délai le Bénéficiaire si une action exécutée au titre des présentes est susceptible d'avoir impacté la disponibilité ou l'intégrité de l'un de ses Systèmes d'information ;
- à avertir ou faire avertir le Bénéficiaire dans les meilleurs délais en cas de découverte, pendant l'Assistance, d'un problème de sécurité majeur pouvant avoir un impact immédiat sur la sécurité de ses Systèmes d'Information ;
- à impérativement solliciter l'accord écrit préalable du Bénéficiaire avant l'exécution de toute action, service ou prestation autre que celles prévues par les présentes et impactant les Systèmes d'Information du Bénéficiaire.

3.2 Obligations du Bénéficiaire

Le Bénéficiaire s'engage pendant toute la durée de l'Assistance :

- à fournir à la demande de l'ANSSI ou du Partenaire des informations exactes notamment concernant les Systèmes d'Information impactés par l'Assistance et les informations relatives aux applications et à leur configuration ainsi que sur les données hébergées ;
- à fournir l'ensemble des éléments pertinents pour apprécier l'existence d'une compromission éventuelle et, le cas échéant, son étendue ;
- de façon générale, à fournir l'ensemble des éléments nécessaires à la réalisation de l'Assistance ;
- à respecter les prérequis à l'installation des équipements de supervision réseau dont la liste est fournie par l'ANSSI ;
- le cas échéant, à transmettre à l'ANSSI son plan de prévention conformément aux articles R. 4512-6 et suivants du Code du travail ;
- à recueillir préalablement l'accord des éventuels tiers, y compris ses filiales, au sens des articles L. 233-1 et suivants du code de commerce, et ses partenaires, dont les Systèmes d'Information sont susceptibles d'être impactés par l'Assistance. Il fournit l'ensemble des justificatifs assurant l'acceptation par les tiers de l'exécution de l'Assistance ;
- à prendre toutes les dispositions nécessaires au respect de la législation et de la réglementation applicable à l'Assistance ;
- à permettre la réalisation des Relevés techniques nécessaires à l'Assistance ;
- à mettre le personnel qui assure la gestion des Systèmes d'Information à disposition pour des entretiens ;

- à informer l'ANSSI ou son Partenaire de toute modification des Systèmes d'Information ou plus généralement, de tout élément susceptible d'impacter l'Assistance ;
- à garantir la sécurité physique du matériel utilisé par l'ANSSI ou le Partenaire dans les locaux du Bénéficiaire ;
- à ne pas utiliser à des fins commerciales ni transmettre à des tiers les outils mis à disposition par l'ANSSI ou le Partenaire et utilisés dans le cadre de l'Assistance ;
- à ne pas utiliser lui-même à des fins internes ces mêmes outils sans accord écrit de la part de l'ANSSI ou du Partenaire.

Le Bénéficiaire permet provisoirement à l'ANSSI et, le cas échéant au Partenaire, aux seules fins de réaliser l'Assistance et sous le contrôle du Bénéficiaire :

- d'accéder et de se maintenir dans ses Systèmes d'Information ;
- de déposer sur ses Systèmes d'Information les outils nécessaires à l'ensemble des actions menées dans le cadre de l'Assistance ;
- d'utiliser toute technique conforme à l'état de l'art afin de procéder à l'Assistance ;
- de recueillir toutes les informations nécessaires aux investigations sur les équipements, à distance depuis les locaux de l'ANSSI ou du Partenaire ou depuis les locaux du Bénéficiaire, à partir des postes de l'ANSSI ou du Partenaire ou ceux du Bénéficiaire. Les agents de l'ANSSI ou du Partenaire indiqueront préalablement à leur exécution les manipulations envisagées aux administrateurs des Systèmes d'Information inclus dans l'Assistance afin qu'ils soient en mesure de juger de leur impact potentiel.

ARTICLE 4 PRESTATIONS D'ASSISTANCE

4.1 Préparation

L'ANSSI et le cas échéant, le Partenaire, avec le concours du Bénéficiaire :

- détermine les modalités techniques de l'Assistance ;
- établit les modalités organisationnelles de l'Assistance (ressources humaines nécessaires, besoins matériels et logistiques).

4.2 Modalités

Le Bénéficiaire met à disposition de l'ANSSI ou du Partenaire un accès direct aux Systèmes d'information impactés par le Signalement aux seules fins de réalisation de l'Assistance.

Le cas échéant, les Parties, identifient les mesures d'urgence à mettre en œuvre de façon immédiate par le Bénéficiaire, afin de limiter le préjudice.

Dans ce cadre, le Bénéficiaire autorise l'ANSSI et, le cas échéant, le Partenaire :

- à procéder à la recherche d'une compromission suspectée ou avérée ;
- à réaliser des collectes d'éléments techniques, à partir de ses réseaux internes et depuis l'extérieur ;
- à effectuer une analyse temps réel ou différée de flux réseau et de systèmes d'équipements informatiques à des fins de supervision de la sécurité, ainsi que d'investigation *a posteriori* sur la base des Relevés techniques. Selon les cas, ces données pourront être traitées chez le Bénéficiaire ou dans les locaux de l'ANSSI ou du Partenaire ;
- à établir les actions de Remédiation nécessaires à la mise en sécurité des Systèmes d'information affectés par l'Incident de sécurité et, le cas échéant, à demander au Bénéficiaire de réaliser lui-même les actions de Remédiation nécessaires afin de remettre le Système d'information en conditions opérationnelles et de sécurité ;
- à s'entretenir avec ses prestataires de service et fournisseurs de solutions intégrées à ses Systèmes d'Information.

Le Bénéficiaire est responsable des informations qu'il transmet aux tiers dans le respect de l'article 11.

Les Parties reconnaissent l'importance de leur collaboration pour mener à bien la réalisation de l'Assistance, objet des présentes.

4.3 Recours à un prestataire qualifié

À l'issue de l'Assistance ou parallèlement à celle-ci, le Bénéficiaire peut faire appel à un prestataire notamment pour l'aider dans la remédiation, la reconstruction ou la sécurisation de son système d'information. L'ANSSI recommande le recours à des prestataires qualifiés au sens du décret n° 2015-350 du 27 mars 2015, modifié, relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information.

Dans ce cas, le recours à un prestataire directement à la demande du Bénéficiaire exclut toute responsabilité de l'ANSSI pour les actions que celui-ci réalise et fait l'objet d'un contrat spécifique entre le Bénéficiaire et son prestataire auquel l'ANSSI n'est pas partie.

ARTICLE 5 PRÉCAUTIONS D'USAGE

L'ANSSI ou le Partenaire prend toutes les précautions utiles pour garantir au Bénéficiaire l'absence de code malveillant connu sur les ordinateurs utilisés. Les outils utilisés par l'ANSSI ou le Partenaire dans le cadre de l'Assistance ne sont pas considérés comme entrant dans cette catégorie.

L'ANSSI ou le Partenaire prend toutes les précautions utiles afin de ne pas porter atteinte au secret des correspondances et à la confidentialité des informations à caractère personnel. Le cas échéant, le Bénéficiaire indique à l'ANSSI ou au Partenaire, les Systèmes d'information susceptibles d'effectuer des traitements de correspondances privées, afin de limiter les risques d'accès à ces informations.

L'ANSSI informe le Bénéficiaire que l'Assistance peut laisser des traces sur ses Systèmes d'Information et notamment au sein des journaux d'administration.

L'ANSSI ou le Partenaire, avec l'aide du Bénéficiaire, prend toutes les précautions utiles afin de limiter les dommages directs ou indirects inhérents à la réalisation de l'Assistance.

Le Bénéficiaire prend les mesures adéquates pour sauvegarder les données contenues au sein de ses Systèmes d'Information, assurer leur conservation préalablement à la mise en œuvre de l'Assistance et préserver l'intégrité et la disponibilité de ses équipements et applications.

Le Bénéficiaire est responsable du fonctionnement de ses Systèmes d'Information et peut refuser ou interrompre à tout moment l'Assistance. À ce titre, il conserve notamment le droit de demander l'interruption à tout moment d'une manipulation quand celle-ci présente un risque inacceptable pour son matériel, son personnel, ses données ou l'une de ses ressources. Cette interruption a pour effet de suspendre la manipulation concernée et non l'Assistance.

Le Bénéficiaire déclare et garantit disposer de tous les droits sur les Systèmes d'Information faisant l'objet de l'Assistance, y compris sur les applications et les données hébergées, sous réserve des droits des tiers.

Le Bénéficiaire s'assure que d'éventuels tiers intervenant dans les Systèmes d'information impactés par le ou les Incidents de sécurité respectent les obligations décrites aux présentes et notamment les obligations de confidentialité. L'ANSSI se réserve le droit de refuser la présence de tiers pour toute partie de l'Assistance si elle l'estime nécessaire.

Le Bénéficiaire est conscient que l'ANSSI ou le Partenaire, aux fins de réaliser l'Assistance, peut involontairement et en dépit des précautions prises :

- entraver ou fausser le fonctionnement des Systèmes d'Information du Bénéficiaire, voire des systèmes d'information de ses partenaires en cas de mutualisation de moyens ou d'interconnexion ;
- introduire, extraire, détenir, supprimer ou modifier des données de ses Systèmes d'Information.

ARTICLE 6 DONNÉES COLLECTÉES

Les Parties s'engagent à respecter la réglementation applicable et notamment celle relative à la protection des données à caractère personnel et au secret des correspondances privées et, le cas échéant, celle relative à la protection des données relevant du secret de la défense nationale.

Le Bénéficiaire garantit un accès aux données concernées par l'Assistance.

À la demande du Bénéficiaire, l'ANSSI ou le Partenaire peut lui fournir une copie des données collectées.

Le Bénéficiaire reconnaît et accepte que l'ANSSI est susceptible d'utiliser les Relevés techniques issus de l'Assistance, dans le cadre de ses missions et sous réserve de les avoir décorrélés du Bénéficiaire sans que cela s'analyse en une rupture de confidentialité.

ARTICLE 7 CORRESPONDANTS

L'ANSSI et, le cas échéant le Partenaire, et le Bénéficiaire s'engagent chacun à fournir au minimum un correspondant disponible pendant toute la durée de l'Assistance.

ARTICLE 8 NOTIFICATION DE FIN D'ASSISTANCE

À l'issue de l'Assistance, l'ANSSI notifie la fin de l'Assistance.

L'ANSSI ou le Partenaire peut fournir un livrable de fin d'Expertise au Bénéficiaire. Ce livrable peut prendre toute forme. L'ANSSI et le Partenaire s'engagent à ne pas diffuser ces livrables en dehors des Parties et des autorités compétentes.

ARTICLE 9 RESPONSABILITÉS

Le Bénéficiaire reconnaît avoir été avisé des risques de dommages, directs et indirects, inhérents à la réalisation de l'Assistance et notamment des dommages qui pourraient en résulter sur ses Systèmes d'Information.

La responsabilité de l'ANSSI et le cas échéant du Partenaire, pourra être engagée uniquement pour les dommages directs subis, pendant l'Assistance, par les Systèmes d'Information du Bénéficiaire, objets de l'Assistance, qui résultent du non-respect par celle-ci des obligations qui lui incombent au titre de l'article 3 des présentes conditions générales.

L'ANSSI et le cas échéant le Partenaire, n'est pas responsable des dommages indirects, lesquels comprennent notamment la perte d'exploitation, les pertes ou disparitions de données non sauvegardées par le Bénéficiaire, le cas échéant le manque à gagner et la baisse de chiffre d'affaires ou le préjudice d'image.

ARTICLE 10 FORCE MAJEURE

Les Parties ne peuvent être tenues pour responsables de l'inexécution (totale ou partielle) ou de retard dans l'exécution des obligations des présentes dans les cas où ceux-ci résultent de circonstances de force majeure au sens de la loi et de la jurisprudence.

ARTICLE 11 CONFIDENTIALITÉ

Sont considérés comme confidentiels les informations, données et documents, quels qu'en soient la nature et l'objet, dont les Parties ont eu connaissance dans le cadre des présentes, par quelque moyen que ce soit, sur quelque support que ce soit, par écrit ou oralement, les éléments relevant de la propriété intellectuelle de l'une ou l'autre des Parties, les Relevés techniques qui n'ont pas été décorrélés du Bénéficiaire. L'intervention de l'ANSSI ou du Partenaire est confidentielle.

Chacune des Parties s'engage :

- à ne communiquer les informations, données et documents confidentiels qu'aux seuls membres de son personnel qui sont dans la nécessité de les connaître pour l'exécution de l'Assistance ;
- à prendre les mesures nécessaires qu'elle-même prend à l'égard de ses propres informations ou données confidentielles pour empêcher la communication ou la divulgation à des tiers.

En application des règles du Code civil relatives au droit à l'image et afin de garantir la sécurité des personnels qui interviennent au titre de l'Assistance, il est rappelé qu'il est interdit de publier des photos des agents de l'ANSSI et le cas échéant des personnels du Partenaire sans leur consentement exprès. Les personnels peuvent s'opposer à toute prise de photographie ou vidéo les incluant.

Les Parties s'engagent expressément à faire respecter à l'ensemble des personnels intervenant lors de l'Assistance (personnel propre et personnel des Partenaires notamment), quel que soit leur statut, la même obligation de confidentialité pour l'ensemble des éléments visés ci-dessus lorsqu'ils y ont accès.

À l'exception de toute information relevant du secret de la défense nationale, les Parties stipulent de manière expresse que ne sera pas considérée comme confidentielle, toute information :

- dont la Partie avait connaissance avant communication par la première Partie ;
- qui fait partie du domaine public ;
- qui a été divulguée par un tiers ayant le droit de le faire.

Par exception, les Marqueurs et Signatures, les traces d'activité de l'attaquant ainsi que les codes malveillants peuvent être réutilisés après l'Assistance et divulgués dans

le respect des règles de partage associées à chacun d'entre eux. En l'absence de telles règles de partage, ceux-ci ne peuvent être rediffusés.

Lorsqu'une Partie constate ou soupçonne une rupture de confidentialité d'une information confidentielle échangée dans le cadre de l'Assistance, elle informe sans délai l'autre Partie et lui précise les circonstances de cette compromission suspectée ou avérée. Les Parties décident alors conjointement des mesures à prendre.

Les Parties peuvent être amenées à échanger des informations protégées par le secret de la défense au sens de l'article 413-9 du Code pénal. Dans ce cas, il sera fait application de la réglementation en vigueur, notamment de l'arrêté du 9 août 2021 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale. Chaque Partie s'engage à désigner à l'autre Partie les personnels ayant l'habilitation prévue par la réglementation qui pourront avoir accès à ces informations.

L'ANSSI ou le Partenaire s'engage à ne communiquer aucune information, même partielle, collectée ou relative au Système d'Information du Bénéficiaire sans son accord préalable écrit.

Cet article ne s'oppose pas à la communication d'informations, sous quelque forme et de quelque nature que ce soit, que l'ANSSI est tenue de faire aux autorités compétentes.

Les Parties s'engagent à respecter les obligations de confidentialité prévues par les présentes pendant toute la durée de l'Assistance et pendant une durée de cinq (5) ans à compter de la fin de l'Assistance.

ARTICLE 12 RÉVERSIBILITÉ

Au terme de l'Assistance, l'ANSSI ou le Partenaire s'engage à supprimer lorsque cela est techniquement possible l'ensemble des outils qui auraient pu être déposés sur le Système d'Information.

L'ANSSI ou le Partenaire remet au Bénéficiaire, dans la mesure du possible, l'ensemble des matériels appartenant au Bénéficiaire qu'elle a reçu pour la réalisation de l'Assistance.

L'ANSSI ou le Partenaire reprend, à l'issue de l'Assistance, l'ensemble des matériels mis en place.

Le Bénéficiaire s'assure que les droits et autorisations accordés aux agents de l'ANSSI ou aux salariés du Partenaire qui intervient pour son compte sont supprimés et qu'il a pris les mesures nécessaires pour que les manipulations opérées sur le Système d'Information au terme de l'Assistance ne puissent plus être imputées à l'ANSSI ou au Partenaire.

ARTICLE 13 COMMUNICATION

Toute communication officielle est décidée d'un commun accord et les éléments de langages sont préparés conjointement par les Parties.

ARTICLE 14 CONDITIONS FINANCIÈRES

Les frais engendrés par la réalisation de l'Assistance objet des présentes sont à la charge de l'ANSSI.

La mise en œuvre et le coût des recommandations faites par l'ANSSI et le cas échéant par le Partenaire, sont à la charge exclusive du Bénéficiaire.

ARTICLE 15 PROPRIÉTÉ

Chaque Partie conserve la propriété de tout élément matériel, logiciel, y compris les Informations confidentielles, mis à disposition de l'autre Partie pour la réalisation de l'Assistance. Aucun transfert de propriété n'est prévu au titre des présentes.

L'ensemble des livrables remis au cours de l'Assistance, quel que soit leur forme (rapports, compte-rendu, livrable

de fin de prestation...) reste la propriété de l'ANSSI ou du Partenaire.

L'ANSSI ou le Partenaire concède au Bénéficiaire un droit d'utilisation exclusif sur le livrable de fin d'Expertise pendant toute la durée des droits d'auteur et sur le monde entier.

ARTICLE 16 MODIFICATION

Toute modification des Conditions générales de Réponse à Incident fera l'objet d'une notification au Bénéficiaire et sera applicable trente (30) jours calendaires après ladite notification, sauf résiliation de sa part.

ARTICLE 17 LITIGES

En cas de litige découlant de l'interprétation ou de l'exécution des présentes, les Parties s'engagent à rechercher une solution amiable. En l'absence d'accord, le traitement du contentieux relèvera de la compétence du tribunal administratif de Paris.