PROCEDURE DES EXAMENS EN DISTANCIEL

I/ PREAMBULE :

ABCIDIA CERTIFICATION organise des sessions d'examen en distanciel sauf pour :
- les épreuves théoriques du domaine énergie (DPE et Audit énergétique),
- l'épreuve pratique AUDIT ENERGETIQUE,
- l'épreuve pratique DPE avec et sans mention à partir du 01/01/2026,

Ces épreuves sont obligatoirement réalisées en présentiel.

L'examen de certification (ou l'examen cas test) en distanciel se présente sous la même forme qu'en présentiel (examen théorique et/ou pratique) via une plateforme sécurisée d'ABCIDIA Certification.

Une télésurveillance des candidats est maintenue durant toute la durée des épreuves.

Pour passer son examen, le candidat peut utiliser son propre ordinateur, à condition que celui-ci fonctionne sous un système d'exploitation WINDOWS.

I/ MOYENS MIS EN PLACE PAR ABCIDIA CERTIFICATION

ABCIDIA Certification met à disposition du candidat un(e) surveillant(e) de session présent(e) et joignable durant toute la durée des épreuves théoriques et pratiques.

Le (la) surveillant(e) de session aura à sa disposition un local adapté de façon à garantir la tranquillité de l'examen.

ABCIDIA Certification mettra à la disposition du (de la) surveillant(e) de session un ordinateur disposant d'une caméra en bon état de fonctionnement, ainsi que d'une bonne connexion Internet afin de limiter tout risque de disfonctionnement informatique pendant l'examen.

En cas de disfonctionnement informatique, le (la) surveillant(e) de session disposera du numéro de téléphone du (ou des) candidat(s) présent(s) à la session de certification de façon à pouvoir communiquer avec lui (ou eux), et de décider des suites à porter à l'examen (suspension temporaire de 15 minutes maximum ou report) selon le disfonctionnement rencontré.

SECURISATION DES FICHIERS « SUJETS » d'examens :

Les fichiers des sujets ainsi que l'ensemble des documents de session seront déposés sur le serveur dédié aux examens de certification. Ces documents ne seront accessibles que par le (la) surveillant(e) de session.

Le candidat aura un lien de connexion au serveur sur un espace personnel qui lui sera attribué. Il ne pourra en aucun cas accéder à son espace sans l'intervention du surveillant de session qui détient le mot de passe d'accès à l'espace. Le mot de passe est changé à chaque nouvelle session de certification en distanciel. Ainsi en cas d'enregistrement fortuit de ce dernier, aucune personne extérieure à ABCIDIA CERTIFICATION ne pourra accéder à l'espace d'un candidat ultérieurement à la session d'examen.

Les fichiers sujets seront déposés par le (la) surveillant(e) de session sur les espaces personnels de chaque candidat, une sécurisation de ce serveur étant paramétrée :

- Impossibilité pour le candidat de se connecter au serveur sans le mot de passe que seul le personnel d'ABCIDIA CERTIFICATION détient. Il n'est en aucun cas communiqué au candidat.

- Dépôt et retrait des fichiers sujets sur le profil de chaque candidat fait par le (la) surveillant(e) de session.
- Possibilité de retrait des fichiers en cours d'épreuve ou de déconnexion au serveur d'un candidat en cas d'attitude contraire aux consignes données (cas de fraude, communication avec d'autres candidats…).
- A la fin de chaque épreuve le (la) surveillant(e) récupère le fichier qui sera définitivement supprimé sur le profil du candidat (impossibilité de ré ouvrir une copie postérieurement à l'épreuve).
- Les fichiers sujets mis à disposition du candidat sur le serveur ne pourront pas être téléchargés sur le PC du candidat.

En outre il sera impossible et interdit de tenter de procéder aux opérations suivantes :
- Capture d'écran de la plateforme.

II/ MOYENS REQUIS POUR LE CANDIDAT :

Le candidat à la certification à distance **doit impérativement** disposer lors de son examen de **l'ensemble** des moyens suivants :

- D'un **ordinateur sous système d'exploitation Windows** mis à jour (pas de MAC sous OS, linux ou autre…) avec WEB CAM et micro intégré ou branché sur lequel il aura préalablement téléchargé l'application de visio conférence indiquée par ABCIDIA Certification (de type « Teamviewer » avec autorisation d'accès de l'application au micro et à la caméra de l'ordinateur ou tablette-pc).

- D'une connexion internet fiable (débit minimum de 30 mégas) : privilégier les connexions filaires à la Wi-Fi quand cela est possible.

- D'un réseau téléphonique de qualité suffisante pour recevoir les appels du surveillant de session.

- D'un local où il pourra s'isoler de façon :
  - d'une part à ne communiquer avec aucune personne extérieure à l'examen (du surveillant de session) ne pourra être que son seul et unique interlocuteur durant toute la durée de l'épreuve) ;

  - et, d'autre part afin de ne pas être perturbé par des interactions extérieures à l'examen en cours d'épreuve.

  L'ensemble de ces moyens réunis sont exigés, l'un de ces moyens ne pourra pas se substituer à un autre, de quelque façon que ce soit.

  Le candidat devra attester, lors de son inscription à l'examen, qu'il disposera des moyens précités le jour de l'examen.

  Si l'un de ces éléments venait à manquer (débit insuffisant, caméra absente ou ne fonctionnant pas… Le surveillant de session annulera de plein droit les épreuves du candidat).

III/ DEROULEMENT DE L'EPREUVE

1/ Dispositions à prendre avant la tenue de l'examen

La semaine précédant son examen, le candidat recevra par mail une convocation à son examen au(x) jour(s) et heure(s) prévus par ABCIDIA Certification, ainsi que la procédure avec les paramétrages indispensables à faire sur son poste avant le jour de l'examen. Ce mail contient également en pièce jointe un lien de connexion au serveur d'examen d'ABCIDIA certification.

Les réglages des applications indiquées devront impérativement avoir été effectués AVANT la session (version, mises à jour éventuelles à vérifier, fonctionnement des micros et caméras), ces réglages entrainant des retards qui auront un impact sur la durée des épreuves.

L'ordinateur du candidat devra être branché sur secteur afin de limiter le risque de panne de batterie, et la batterie de son téléphone portable devra être chargée pour permettre au surveillant de session de le contacter.

Tout retard de plus de 10 (dix) minutes entrainera soit le report de l'examen à une date, ou à un horaire ultérieur(e) en fonction des disponibilités de ABCIDIA Certification.
Le candidat est par conséquent appelé à être ponctuel afin de s'assurer les meilleures conditions de réussite à son examen.

2 / Déroulement de l'examen

Le candidat devra, tout au long des épreuves, suivre les consignes et répondre aux demandes du (de la) surveillant(e) de session. A défaut, le surveillant de session pourra mettre fin à la session de certification unilatéralement et sans avertissement préalable.
De même, tout candidat qui outrepassera les règles ci-dessous énoncées pourra se voir être ajourné temporairement ou définitivement sur décision d'**ABCIDIA Certification.**

A / CONTROLE DE L'IDENTITE DES CANDIDATS

En début de session d'examen, le (la) surveillant(e) de session contactera chaque candidat individuellement l'un après l'autre.

Tout candidat ne répondant pas au bout de deux tentatives d'appel du (de la) surveillant(e) de session sera considéré absent.

Dès lors que le candidat sera connecté à la réunion en visioconférence, le surveillant de session pourra procéder à son contrôle d'identité (présentation d'un justificatif d'identité : CNI, passeport, ou tout autre titre d'identité officiel comportant sa photo) en le positionnant devant la caméra de telle façon que le (la) surveillant(e) de session puisse voir clairement le document et contrôler l'identité du candidat.

B/ VERIFICATION DES MOYENS TECHNIQUES DU CANDIDAT

Lors de l'appel téléphonique du (de la) surveillant(e) de session, le candidat devra fournir son identifiant et un mot de passe généré par l'application de visio/contrôle des postes qu'ABCIDIA Certification aura préalablement indiqué au candidat, afin de prendre la main sur le poste du candidat.

Dès lors, le surveillant de session pourra contrôler que le poste du candidat regroupe bien l'ensemble des moyens techniques requis. Il pourra notamment effectuer un test de vitesse de débit internet si la connexion lui semble limitée.

Le (la) surveillant(e) de session connectera le candidat à la réunion de visio conférence. Il connectera ensuite le candidat au serveur d'ABCIDIA Certification sur lequel le candidat effectuera son épreuve.

Si, lors de cet appel téléphonique, le (la) surveillant(e) de session constate que le candidat n'a pas préparé son ordinateur, il pourra mettre fin immédiatement à la procédure d'examen et annuler la session de certification du candidat quitte à la remettre à une date ultérieure, lorsque les moyens seront réunis.

Le candidat à la certification en distanciel autorise de plein droit ABCIDIA Certification à prendre le contrôle de son poste informatique, d'y effectuer les paramétrages et réglages nécessaires à la réalisation de ses examens à distance (installation de programmes informatiques, lancement de mises à jour d'outils…) de consulter des pages internet telles que les tests de débit internet, d'avoir accès à la boîte mail des candidats (pour l'ouverture de la pièce jointe – outils de connexion au serveur).

C/ GESTION DU RISQUE DE FRAUDE

Après contrôle satisfaisant des moyens techniques du candidat, le (la) surveillant(e) de session pourra procéder, toujours lors de cet appel téléphonique au contrôle de l'environnement de travail du candidat via sa web cam, afin d'éviter tout risque de fraude. En outre, seront vérifiés les points suivants :

- Le candidat devra être seul dans un local qu'il aura prévu à cet effet de sorte qu'il ne pourra communiquer avec personne d'autre que le (la) surveillant(e) de session pendant toute la durée de l'examen.

- Pour les épreuves sans documentation autorisée, le surveillant pourra procéder à une inspection des abords directs du poste de travail du candidat afin de valider le respect de ces consignes. Le candidat devra par ailleurs faire son épreuve sur le même écran que celui où est positionné sa caméra. Le (la) surveillant(e) de session pourra ainsi contrôler que le candidat reste bien face à son sujet et ne consulte aucun support.

- Toute **utilisation de logiciel professionnel ou application métier est interdite** sauf pour **les examens cas tests DPE** qui font suite à une opération de surveillance documentaire ou à un contrôle sur ouvrage. Lors de ce type d'examen, il est fortement conseillé au candidat de se munir de deux écrans : l'un sur lequel l'énoncé sera mis à sa disposition, l'autre sur lequel il pourra saisir et réaliser le DPE du bien objet du cas test, sur son propre logiciel.

Toute non-conformité entrainera l'annulation de l'examen.

Le contrôle de l'environnement de travail du candidat pourra être répété de façon aléatoire, autant de fois que le (la) surveillant(e) de session le jugera nécessaire et durant toute la durée des épreuves. Le candidat qui refusera ce contrôle ou qui ne répondra pas à l'appel de le (la) surveillant(e) de session sera automatiquement ajourné de son épreuve. Le (la) surveillant(e) de session lui coupera l'accès à la plateforme. Le candidat est par conséquent enjoint à garder son téléphone à proximité de son poste de travail.
Il devra montrer son environnement de travail sans délais dès lors que cette demande lui aura été formulée.

Toute tentative de repousser ce contrôle pourra entraîner la suspension de l'épreuve et l'ajournement du candidat.

En dehors des contrôles de l'environnement de travail, le candidat **devra rester de façon permanente dans le champ de la caméra.**

Ainsi le candidat ne pourra pas s'absenter de son poste de travail durant l'examen pour quelque motif que ce soit, sauf cas d'urgence avec autorisation du (de la) surveillant(e) de session.

Si le (la) surveillant(e) de session s'aperçoit que le candidat communique avec une tierce personne, de quelque façon que ce soit, et sur quelque sujet que ce soit, l'ajournement sera prononcé.

Le téléphone du candidat devra de préférence rester en mode « vibreur » afin de répondre aux appels aléatoires du (de la) surveillant(e) de session. Toutefois, tout autre appel, message etc. que le candidat pourrait recevoir de l'extérieur durant l'examen ne pourra être consulté et aucune réponse ne pourra être faite durant l'épreuve. Le (la) surveillant(e) de session veillera au respect de ces consignes et tout manquement entrainera l'ajournement du candidat, sauf cas d'urgence avec autorisation du (de la) surveillant(e) de session).

Au cours des épreuves, le (la) surveillant(e) de session aura un accès permanent au visuel du poste du candidat afin d'être en mesure de le guider dans son épreuve. Cet accès se limitera à la consultation des copies et en aucun cas le (la) surveillant(e) de session ne pourra modifier quelque fichier que ce soit.

Lorsque la durée de l'épreuve sera écoulée, le candidat sera invité à se relire, puis à enregistrer son travail et à fermer le fichier « sujet ». Le candidat devra s'exécuter sans délais. A défaut, le (la) surveillant(e) de session pourra intervenir sur l'espace du candidat et forcer la fermeture du fichier. Tout abus pourra entrainer des sanctions à l'encontre du candidat. Toutefois, l'accès à l'espace candidat étant limité en temps et en heures, une coupure automatique sera réalisée. L'enregistrement du fichier, pour les modifications effectuées après la fin de l'épreuve annoncée, ne sera pas garanti.

L'application «Teamviewer* » est citée à titre d'exemple et n'est pas sélectionnée de façon définitive, ABCIDIA CERTIFICATION se réservant la possibilité de changer de mode ou d'application de communication.

3/ Contenu de l'examen

a) Certification initiale

L'examen de certification initiale à distance est composé d'une épreuve théorique et d'une épreuve pratique pour chacun des domaines de certification. Chaque épreuve répond aux exigences des textes règlementaires à savoir :

- Arrêté du 1er juillet 2024 pour les domaines gaz, électricité, plomb avec et sans mention, amiante avec et sans mention, termites ;
- Arrêté du 20 juillet 2023 pour le DPE avec et sans mention (uniquement les épreuves pratiques et jusqu'au 01/01/2026);

Ces épreuves sont identiques à celles passées en présentiel.

b) Renouvellement de certification (tous domaines sauf énergie)

L'examen de renouvellement de certification est composé d'une épreuve pratique faisant suite à un examen documentaire.

Ces épreuves sont identiques à celles passées en présentiel.

Pour le domaine énergie, le renouvellement se réalise sans examen, conformément aux dispositions règlementaires (voir les règlements techniques d'évaluation concernés).

IV/ CONDUITE A TENIR EN CAS DE DISFONCTIONNEMENT

En cas de disfonctionnement informatique, le (la) surveillant(e) de session contactera le candidat par téléphone afin de savoir ce qu'il en est. Le candidat devra donc s'assurer d'avoir une couverture téléphonique suffisante pour recevoir l'appel du (de la) surveillant(e) de session.
S'il s'agit d'une simple mise à jour, paramétrage, réglage ou toute autre action pouvant être menée sous 15 (quinze) minutes maximum, l'examen pourra se tenir et la durée des épreuves n'en sera pas affectée. La suspension temporaire de la session sera accordée sur autorisation du (de la) surveillant(e) de session

Passé le délai de 15 (quinze) minutes, si la connexion n'est pas rétablie, le (la) surveillant(e) de session pourra reporter l'examen à une date ou à un horaire ultérieur(e) en fonction des disponibilités de **ABCIDIA Certification**.

En cas de bug en cours d'épreuve, le (la) surveillant(e) de session notera l'heure de survenance de l'incident afin de déterminer le temps restant au candidat pour son épreuve.

V/ ACCORD MUTUEL PREALABLE DE SECURISATION DES INFORMATIONS ET DE PROTECTION DES DONNEES

Pour mener à bien les examens en distanciel, **ABCIDIA Certification** demande au candidat d'utiliser un logiciel qui permet au (à la) surveillant(e) de session de prendre le contrôle de son poste informatique.

Cette mise à disposition du poste du candidat entraîne la possibilité pour **ABCIDIA Certification** d'avoir accès fortuitement à des données personnelles du candidat, bien que le (la) surveillant(e) de session) ne se limite qu'à des manipulations nécessaires à la tenue de la session d'examen (accès aux historiques de téléchargement, historiques de navigation internet, boite mail…).

ABCIDIA Certification ne pourra être tenue responsable de toute perte, endommagement de fichier, modification ou autre de donnée(s) sur le poste de candidat.

ABCIDIA Certification s'engage à respecter la confidentialité des données auxquelles elle pourra avoir accès dans le cadre de sa mission, et à se limiter aux manipulations informatiques nécessaires à la tenue des examens en distanciel.

Ces dispositions sont reprises sous la forme d'un accord mutuel que le candidat s'engage à signer lors de son inscription à l'examen (accord intégré dans le dossier de candidature).

VI/ POLITIQUE DE CONFIDENTIALITE ET SECURITE DES DONNEES

Confidentialité et Protection des données personnelles

Périmètre d'application
Nous nous engageons à vous fournir des produits et services de qualité, de manière professionnelle, tout en protégeant votre vie privée.
La présente politique de confidentialité s'applique à tous les services d'ABCIDIA, les applications, outils et services (collectivement "Services") pour lesquels cette politique est publiée, quel que soit le moyen par lequel vous y accédez et les utilisez.
Cette politique s'applique aussi à toutes autres formes de communication que nous échangeons avec vous.

Contact
Pour toute question ou plainte relative à notre politique de confidentialité, ou nos pratiques de traitement de l'information, vous pouvez joindre à la société ABCIDIA en écrivant à l'adresse suivante : ABCIDIA Domaine de Saint Paul - Bat : A6 - 4e étage - 102, route de Limours
78470 Saint-Rémy-lès-Chevreuse - Tél : **01 30 85 25 71.**
Notre équipe assurant le respect de la confidentialité et de la protection des données est également à votre disposition par email : contact@abcidia-certification.fr.

Informations personnelles que nous collectons
Si vous participez à une certification, votre employeur (ou un autre tiers payant pour la formation ou certification) nous fournit les coordonnées de votre entreprise : nom, adresse électronique, adresse physique et numéro de téléphone. Certains employeurs fournissent également des informations d'identification supplémentaires, telles qu'un numéro d'identification d'employé. Nous ne demandons ni ne traitons des informations personnelles sensibles.

Si vous achetez une certification pour vous-même ou que vous interagissez avec nos Services sans être participant, nous collectons les informations de contact que vous fournissez.

En interagissant avec nos services, nous collectons l'adresse IP. Nous générerons également des informations sur votre utilisation des services, y compris la création de l'enregistrement de votre certification.

Nous ne considérons pas les informations comme personnelles si celles-ci incluent des informations anonymisées ou agrégées, de sorte qu'elles ne peuvent plus être utilisées pour identifier une personne physique spécifique, même en combinaison avec d'autres informations.

Informations d'identification telles que nom, adresse, numéro de téléphone et adresse e-mail lorsque vous vous inscrivez à une certification.

Autres contenus que vous générez ou qui sont connectés à votre compte (tels que votre historique de certification, votre progression sur un module en ligne, et vos préférences utilisateur)

Routage, facturation et autres informations utilisées pour envoyer des factures ou autres informations.

Vous pouvez nous fournir d'autres informations dans de nombreux autres cas : via une adresse mail : contact@abcidia-certification.fr, en mettant à jour ou en ajoutant des informations liées à

votre profil, en participant à certaines discussions des communautés instituées par ABCIDIA, pour régler un différend, ou lorsque vous échangez avec nous sur nos prestations de services.

Des informations supplémentaires peuvent vous être demandées que nous sommes tenus ou autorisés par les lois nationales à collecter et à traiter afin de vous authentifier ou de vous identifier ou de vérifier les informations que nous avons collectées.

Informations personnelles que nous collectons automatiquement lorsque vous utilisez nos Services :
Nous recueillons des informations sur votre interaction avec nos services. Ce sont les informations que nous recevons des appareils (y compris les appareils mobiles) que vous utilisez lorsque vous accédez à nos services. Ces informations peuvent inclure les éléments suivants : ID de périphérique ou identifiant unique, type de périphérique et jeton de périphérique unique
Informations sur l'ordinateur et la connexion, telles que les statistiques sur vos pages vues, le trafic depuis et vers les sites, l'URL de référence, les données d'annonce, votre adresse IP.

Informations personnelles collectées via d'autres sources
Comme décrit ci-dessus, nous recueillons des informations de contact auprès des employeurs et des tiers qui effectuent des demandes de certification.
Nous pouvons être amenés à compléter les informations personnelles que nous recueillons et les ajouter à vos informations de compte, comme par exemple des informations démographiques et autres informations accessibles au public selon la juridiction.

Quand les informations sont-elles collectées ?
Nous recueillons des informations lorsque vous utilisez nos Services. Nous recueillons également des informations personnelles vous concernant et tout appareil (y compris les appareils mobiles) que vous utilisez lorsque vous passez une certification. Mettre à jour ou ajoutez des informations à votre compte, fournissez des informations d'un autre événement, ou lorsque vous correspondez avec nous.
Nous recueillons également des informations lorsque des commandes vous concernant sont passées directement par vous ou des tiers (votre employeur, ou une organisation tierce achetant des services en votre nom).

Vos choix sur la façon dont nous utilisons vos informations personnelles
Nous nous efforçons de vous fournir des choix sur la manière dont nous utilisons vos informations personnelles pour communiquer avec vous, pour vous envoyer des informations sur votre suivi de certification et sur la manière dont nous vous fournissons des services personnalisés et des informations pertinentes.

Il existe toutefois des cas où le traitement de vos informations peut être limité ou déterminé par d'autres. Si vos données nous ont été fournies par votre employeur (ou une autre partie payant pour vos services), nous traiterons les données en fonction des intérêts légitimes de votre employeur à vous fournir des services dans le cadre de cette relation. Nous pouvons également traiter vos informations personnelles dans notre intérêt pour la conformité et la tenue des registres commerciaux. Vous avez le droit de vous opposer au traitement de vos informations personnelles dans ces circonstances en nous contactant à l'adresse contact@abcidia-certification.fr.

Comment nous utilisons vos informations personnelles
Nous utilisons vos informations personnelles pour fournir et améliorer nos services, vous fournir une expérience personnalisée dans l'utilisation de nos services, vous contacter au sujet de votre compte et de nos services, vous fournir un service client, et enquêter sur des activités frauduleuses ou illégales.

Si nous avons reçu vos informations personnelles d'un employeur en relation avec la fourniture des Services, nous utiliserons ces informations pour communiquer avec vous et fournir les

Services. Nous pouvons également fournir des informations sur votre utilisation des Services à votre employeur.
Des informations sur les services fournis à une personne déterminée peuvent apparaître dans les factures et autres documents financiers. Nous pouvons également traiter et conserver des informations personnelles à des fins de conformité avec les lois et réglementations.

Accès, contrôle et corrections de vos informations personnelles
Nous respectons votre droit d'accès, de rectification, de demande de suppression ou de restriction d'utilisation de vos informations personnelles, conformément à la législation en vigueur. Nous prenons également des mesures pour nous assurer que les informations personnelles que nous recueillons sont exactes et à jour.
Vous avez le droit de savoir quelles informations personnelles nous conservons à votre sujet
Nous vous fournirons une copie de vos informations personnelles dans un format structuré, communément utilisé et lisible sur demande.
Si vos informations personnelles sont incorrectes ou incomplètes, vous avez le droit de nous demander de les mettre à jour.
Vous avez le droit de vous opposer au traitement de vos informations personnelles
Vous pouvez également nous demander de supprimer ou de restreindre l'utilisation de vos informations personnelles, mais ce droit est déterminé par la loi applicable et peut avoir un impact sur votre accès à certains de nos services.

Partage de vos informations personnelles
Nous pouvons être amenés à divulguer vos informations personnelles à d'autres entreprises comme le ministère pour le transfert de vos compétences. Cette divulgation peut être nécessaire pour que nous vous fournissions l'accès à certains de nos services, pour respecter nos obligations légales, pour appliquer nos conditions générales ou d'autres accords, pour faciliter nos activités de certification ou pour prévenir, détecter, atténuer et enquêter sur les activités frauduleuses ou illégales liées à nos services et se conformer à la loi. Nous essayons de minimiser la quantité d'informations personnelles que nous divulguons à ce qui est directement pertinent et nécessaire pour atteindre l'objectif spécifié.
Nous ne vendons, louons ou divulguons vos informations personnelles à des tiers à des fins de marketing et de publicité sans votre consentement.

Durée de conservation de vos données personnelles
Nous conservons vos informations personnelles aussi longtemps que nécessaire pour fournir les Services, ou à d'autres fins essentielles, telles que la tenue des registres au ministère, le respect de nos obligations légales, la résolution des litiges et l'application de nos règles.

Protection de vos données personnelles
Nous protégeons vos informations personnelles en utilisant des mesures de sécurité techniques et administratives afin de réduire les risques de perte, d'utilisation abusive, d'accès non autorisé, de divulgation et de modification. Certaines des mesures de protection que nous utilisons sont les pares-feux et le cryptage des données, les contrôles d'accès physique à nos centres de données et les contrôles d'autorisation d'accès à l'information.

CONNEXION ET REGLES DE PROTECTION DES DONNEES AVEC TEAMVIEWER

Datacenters et dorsale

Tous les serveurs TeamViewer sont hébergés dans des datacenters sécurisés et conformes à la norme ISO 27001. De plus, ils utilisent des alimentations électriques redondantes et des connexions de porteurs à multi-redondance. Elles incluent la protection des données de l'ensemble RAID, la mise en miroir et la sauvegarde des données, le stockage sur serveur hautement disponible et les systèmes de routeur avec des mécanismes de récupération d'urgence, ainsi que des procédures mises en place pour offrir un service continu. De plus, tous les serveurs qui stockent des données sensibles se trouvent en Allemagne ou en Autriche.

Les datacenters ont implémenté des contrôles dernier cri en matière de sécurité, c'est-à-dire le contrôle de l'accès personnel, la vidéosurveillance, les détecteurs de mouvement, ainsi que la surveillance 24 heures sur 24 et 7 jours sur 7. Par ailleurs, le personnel de sécurité sur site vérifie que l'accès au datacenter est uniquement accordé aux personnes autorisées et garantit la meilleure sécurité possible pour le matériel et les données. Un contrôle d'identification détaillé est également effectué à l'unique point d'entrée du datacenter.
Signature de code

En guise de fonctionnalité de sécurité supplémentaire, tous nos logiciels sont signés via la signature de code DigiCert. De cette façon, l'éditeur du logiciel est toujours aisément identifiable. Si le logiciel est modifié par la suite, la signature numérique est automatiquement invalidée.
Sessions TeamViewer
L'intégralité du transfert de données de la Management Console s'effectue via un canal sécurisé qui utilise le cryptage TLS (Transport Layer Security), la norme pour les connexions réseau Internet sécurisées. Pour l'authentification et le cryptage du mot de passe, le protocole Secure Remote Password (SRP), un protocole de concordance de clé authentifiée par mot de passe (PAKE) augmenté, est utilisé. Un infiltrateur, ou homme du milieu, ne peut obtenir suffisamment d'informations pour deviner un mot de passe par force brute. Cela signifie qu'une sécurité élevée peut être obtenue même avec des mots de passe faibles. Toutefois, TeamViewer recommande de respecter les meilleures pratiques du secteur en matière de création de mots de passe, afin de garantir les niveaux de sécurité les plus élevés.

Chaque client TeamViewer a déjà mis en œuvre la clé publique du cluster maître et peut donc crypter les messages sur le cluster maître et vérifier les messages qu'il a signés. La PKI (Public Key Infrastructure ou infrastructure de clé publique) prévient efficacement les « attaques de l'homme du milieu » (MITM, man-in-the-middle-attacks »). Malgré le cryptage, le mot de passe n'est jamais envoyé directement, mais uniquement par le biais d'une procédure défi-réponse, et est enregistré uniquement sur l'ordinateur local. Lors de l'authentification, le mot de passe n'est jamais transféré directement du fait que le protocole Secure Remote Password (SRP) est utilisé. Seul un vérificateur de mot de passe est stocké sur l'ordinateur local.

CRÉATION D'UNE SESSION ET TYPES DE CONNEXION

Lorsque vous établissez une session, TeamViewer détermine le type de connexion optimal. Après un passage par nos serveurs maîtres, une connexion directe via UDP ou TCP est établie dans 70 % des cas (même derrière des passerelles, NAT et pare-feu standard). Le reste des connexions est acheminé dans notre réseau de routeur hautement redondant via la tunnellisation https ou TCP.

Il est inutile d'ouvrir des ports pour travailler avec TeamViewer.

CRYPTAGE ET AUTHENTIFICATION

Le trafic TeamViewer est sécurisé à l'aide d'un échange de clé publique/privée RSA et d'un cryptage de session AES (256 bits). Cette technologie est utilisée dans une forme comparable pour le protocole https/SSL et est considérée 100 % sécurisée par les normes actuelles.

Comme la clé publique ne quitte jamais l'ordinateur du client, cette procédure garantit que les ordinateurs interconnectés, notamment les serveurs de routage TeamViewer, ne peuvent pas déchiffrer le flux de

données. Les opérateurs des serveurs de routage comme TeamViewer ne peuvent en aucun cas lire le trafic des données cryptées.

Validation d'ID TeamViewer

Les ID TeamViewer s'appuient sur diverses caractéristiques matérielles et logicielles et sont automatiquement générés par TeamViewer. Les serveurs TeamViewer contrôlent la validité de ces ID avant chaque connexion.

Protection contre les attaques par force brute

Les futurs clients qui s'inquiètent de la sécurité de TeamViewer posent souvent des questions sur le cryptage. Et ce à juste titre, car le risque qu'une tierce personne puisse contrôler la connexion ou que les données d'accès à TeamViewer soient exploitées est leur plus grande crainte. Cependant, la réalité, c'est que les attaques plutôt primitives sont souvent les plus dangereuses.

Dans le cadre de la sécurité informatique, une attaque par force brute est une méthode par tâtonnements pour deviner un mot de passe protégeant une ressource. Avec la croissance de la puissance de calcul des ordinateurs standard, le temps nécessaire pour deviner les mots de passe longs a été progressivement réduit.

Pour se protéger contre les attaques par force brute, TeamViewer augmente de plus en plus la latence entre les tentatives de connexion. Ainsi, il ne faut pas moins de 17 heures pour 24 tentatives. La latence est uniquement réinitialisée après avoir correctement saisi le mot de passe adéquat.

TeamViewer intègre non seulement un mécanisme pour protéger ses clients des attaques émanant d'un ordinateur spécifique, mais également de plusieurs ordinateurs, appelées attaques de botnet, qui tentent d'accéder à un ID TeamViewer spécifique.

ARTICLE 1 BASE JURIDIQUE DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

L'ensemble des données personnelles n'est traité qu'avec l'accord explicite du client ou, éventuellement, sans son accord explicite lorsque le traitement mis en œuvre est indispensable à l'exécution d'un contrat que la personne concernée a conclu avec la société ABCIDIA. La conservation des données de connexion du compte client est inscrite dans le cadre de l'obligation légale de tout opérateur de services de communication électronique. L'ensemble des données collectées proviennent directement du client ou de l'utilisateur du service du client.

ARTICLE 2 DONNEES SENSIBLES

Aucune donnée sensible n'est traitée, mais il sera rappelé qu'aucune donnée sensible ne peut être traitée sans le consentement explicite de la personne concernée ou lorsque ces données ont manifestement été rendues publiques par la personne concernée ou encore, lorsque le traitement de ces données est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice.

ARTICLE 3 DROIT D'ACCES, DE RECTIFICATION, D'OPPOSITION, D'EFFACEMENT ET DE VERROUILLAGE DES DONNEES

En application des présentes règles internes, l'ensemble de la société ABCIDIA doit permettre : - De laisser à toute personne le droit d'obtenir une copie de toutes les données traitées la concernant, sans contrainte, à des intervalles raisonnables et sans délai ou frais excessifs, - Le droit, pour toute personne concernée, d'obtenir la rectification, l'effacement ou le verrouillage de données, notamment au motif que les données sont incomplètes ou inexactes, - Le droit, pour toute personne concernée, de s'opposer à tout moment, pour des raisons impérieuses et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf en cas de dispositions contraires du droit national. Dans toutes les hypothèses où l'opposition est justifiée, le traitement doit être interrompu sans délai, - Le droit, pour toute personne concernée, de s'opposer, sur simple demande et sans frais, aux traitements de données à la concernant à des fins de démarchage direct. Ces droits peuvent être exercés auprès du Correspondant Informatique et Libertés de la société ABCIDIA à l'adresse MAIL@abcidia-certification.fr.

ARTICLE 4 DECISION INDIVIDUELLE AUTOMATISEE

La société ABCIDIA s'engage à ce qu'aucune évaluation ou décision en rapport avec la personne concernée et de nature à l'affecter de manière significative ne soit fondée uniquement sur le traitement automatisé de ces données, en dehors des hypothèses où la décision en question est prise en vue de la conclusion ou de l'exécution d'un contrat, à condition que la demande de conclusion et d'exécution des

contrats introduite par la personne concernée ait été satisfaite ou que des mesures appropriées, telles que la possibilité de faire valoir son point de vue, garantissent la sauvegarde de son intérêt légitime.

ARTICLE 5 SECURITE ET CONFIDENTIALITE

La société ABCIDIA et ses filiales prennent l'engagement de prendre l'ensemble des mesures d'ordre technique et organisationnel appropriées, afin de protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé, notamment lorsque le traitement comporte des transmissions de données via un réseau, ainsi que contre toute autre forme de traitement illicite. En particulier, la société ABCIDIA a mis en place, conformément à la politique de sécurité visée à l'annexe 6, les mesures de sécurité suivantes : • Sécurité physique des locaux assurant l'hébergement des serveurs. Cet accès est réalisé par badge d'accès pour toute personne y compris les visiteurs, les intervenants extérieurs, les locaux donnant accès aux serveurs ne sont accessibles que par biométrie, l'accès aux serveurs est limité aux personnes habilitées, • Protection contre les intrusions extérieures utilisant le canal des réseaux informatiques : routeur, par feu, • Mesures destinées à assurer la confidentialité des données : développement de l'application dans un environnement informatique distinct de celui de la production, • Mesures destinées à assurer la confidentialité des données lors des opérations de maintenance des équipements informatiques : intervention de maintenance des matériels enregistrés dans une main courante, support de stockage destiné à la destruction faisant l'objet d'une procédure de formatage bas niveau. • Mesures destinées à assurer la confidentialité des données lors des opérations de maintenance des logiciels informatiques : rédaction d'une charte administrateur, intervention de maintenance des logiciels dans l'environnement de production enregistré par le biais de logs, • Authentification et identification des personnes habilitées à accéder à l'application : accès par mot de passe, définition de profil d'habilitation pour chaque utilisateur en fonction des fonctions autorisées et catégories d'information accessible, accès à l'application faisant l'objet d'une journalisation (date, heure de connexion, identifiant d'utilisateur). • Mise en place de proxy et firewall. • Conservation des supports de stockage en interne même en cas de réparation. • Des mesures particulières sont prises, s'agissant de données bancaires.

ARTICLE 6 RESTRICTION AU TRANSFERT

Aucun transfert de données n'est effectué vers des responsables de traitement ou sous-traitants externes à la société ABCIDIA à l'exception de mesures d'audit (audit de sécurité, notamment) Il s'agit, notamment, du transfert d'informations vers les registres aux fins d'enregistrements des noms de domaine (exemple : auprès de l'AFNIC pour le .fr) et vers le prestataire chargé de la politique SSL pour la protection des données. Ces transferts sont encadrés, dans le cas de transfert hors Union Européenne, par l'utilisation des clauses contractuelles types élaborées par la Commission Européenne afin d'assurer en toutes circonstances un niveau de protection adéquat aux données transférées.