SUMMARY

1. INTRODUCTION

L'objectif principal de cette politique de sécurité de l'information pour les partenaires est de diriger un programme efficace de protection des actifs informationnels, en vue d'assurer la confidentialité, l'intégrité et la disponibilité des informations, et de servir de base à l'établissement de normes et de procédures de sécurité de l'information au sein du groupe WEG.

2. CHAMP D'APPLICATION

Tous les partenaires (toute personne ayant une relation juridique avec le groupe WEG en tant que fournisseur de produits, de licences ou de services) doivent se conformer aux exigences en matière de sécurité de l'information définies dans le présent document.
Le respect des lignes directrices établies est essentiel à l'efficacité de la relation de partenariat signée et à la réalisation de niveaux adéquats de protection de l'information.
Les lignes directrices et les exigences définies dans le présent document s'appliquent à tous les partenaires qui ont accès aux données, aux informations et aux systèmes du groupe WEG. Les partenaires sont responsables d'eux-mêmes et de leurs employés, fournisseurs et prestataires de services.

3. DÉFINITIONS

- **DPIA:** est l'acronyme de Data Protection Impact Assessment (évaluation de l'impact de la protection des données), qui correspond à Personal Data Protection Impact Report (RIPD) dans la loi générale brésilienne sur la protection des données (LGPD). Ce processus permet d'identifier, d'évaluer et d'atténuer les risques pour la vie privée dans les projets de données avant qu'ils ne soient mis en œuvre. Il s'agit d'une responsabilité légale et obligatoire lorsque le traitement des données peut mettre en danger les droits et libertés des personnes concernées.
- **Opt-in:** il s'agit d'un terme anglais qui signifie l'autorisation d'un utilisateur à recevoir des informations de la part d'une entreprise.
- **Opt-out:** ce terme signifie « choisir de quitter », il s'agit d'un mouvement dans lequel l'individu a l'autonomie de cesser de faire partie de quelque chose qui est inséré.
- **Séparation des tâches (SOD) :** Il s'agit d'un principe de contrôle interne qui vise à éviter les risques, tels que la fraude, les erreurs et les cyberattaques, dans les organisations. La séparation des tâches repose sur la délégation des tâches entre différentes personnes ou différents groupes, afin d'éviter qu'une même personne n'exerce un contrôle total sur des systèmes, des processus ou des activités confidentielles.
- **Politique du moindre privilège :** Il s'agit d'un concept de cybersécurité qui consiste à n'accorder aux utilisateurs que le minimum de privilèges nécessaires à l'accomplissement de leurs tâches.
- **Runbooks:** guides détaillés qui décrivent les procédures et les processus d'une organisation, dans le but de garantir que les activités sont exécutées de manière cohérente, sûre et efficace.
- **Durcissement :** processus visant à renforcer la sécurité des systèmes, des réseaux, des logiciels, du matériel, des microprogrammes et des infrastructures informatiques, afin de les rendre plus résistants aux cyberattaques.

- **Patchs de sécurité :** mises à jour correctives visant à corriger les vulnérabilités, les failles et les bugs dans les logiciels et les plateformes. Le mot « patch » est un terme anglais qui signifie « rustine » ou « correctif ».
- **OWASP:** Open Worldwide Application Security Project (OWASP) est une organisation internationale à but non lucratif qui œuvre à l'amélioration de la sécurité des applications web et mobiles. L'OWASP est l'une des principales initiatives de lutte contre la cybercriminalité.
- **Privacy and Security by Design:** concepts qui font référence à la protection des données et à la sécurité des systèmes de manière proactive, dès la conception d'un projet ou d'un service.
- **Phishing:** type de cyberattaque visant à voler des informations personnelles ou à accéder à des comptes en ligne. Les escrocs utilisent des messages frauduleux qui semblent légitimes pour inciter les victimes à révéler des données sensibles.
- **Piratage éthique :** Le hacking éthique est une pratique de sécurité numérique qui consiste à simuler une cyberattaque afin d'identifier et de corriger les vulnérabilités des systèmes, des réseaux ou des applications.
- **Tests de pénétration :** Les tests de pénétration (ou pentesting) sont des attaques simulées autorisées que les organisations effectuent sur leurs propres systèmes ou réseaux informatiques afin d'évaluer leur sécurité. L'objectif est de découvrir les vulnérabilités à l'aide des mêmes outils, techniques et processus que ceux utilisés par les pirates informatiques. En révélant les faiblesses de la cybersécurité, les tests d'intrusion contribuent à réduire les risques de cyberattaques malveillantes..

4. LES RESPONSABILITÉS

4.1. Domaine contractuel des services aux fournisseurs

- Au cours du processus d'embauche des partenaires (y compris les employés, les fournisseurs et les prestataires de services liés au partenaire) qui doivent accéder au réseau interne, aux systèmes, aux informations ou aux données du groupe WEG, la zone contractante doit veiller à ce que toutes les personnes concernées soient informées de la présente politique de sécurité de l'information.
- La zone contractante doit veiller à ce que les contrats avec les partenaires comportent des clauses spécifiques sur la sécurité de l'information et la protection des données, y compris une référence expresse à la présente politique de sécurité de l'information.

4.2. Partenaires

- Il incombe aux partenaires d'observer et de suivre les lignes directrices énoncées dans la présente politique de sécurité de l'information ; et
- Les activités réalisées doivent être conformes à la législation en vigueur et à la normalisation des organismes et entités de réglementation en matière de sécurité de l'information applicables à l'objet du contrat.

5. LIGNES DIRECTRICES

5.1. Général

Les partenaires, qu'ils soient fournisseurs de produits, de licences ou de services, doivent s'engager à respecter pleinement ce qui suit :

- Protéger les informations contre l'accès, la modification, la destruction ou la divulgation non autorisés, tout en préservant leur confidentialité ;
- Veiller à ce que les ressources mises à leur disposition soient utilisées uniquement aux fins approuvées par le Groupe WEG ;
- Veiller à ce que les systèmes et les informations sous sa responsabilité soient protégés de manière adéquate, conformément aux normes du Groupe WEG ;
- Assurer la continuité du traitement des informations commerciales critiques ;
- Respecter les lois et les normes qui régissent les aspects liés à la propriété intellectuelle ;
- mettre en œuvre et maintenir des contrôles de sécurité de l'information, conformément aux meilleures pratiques du marché et aux réglementations applicables ;
- Signaler immédiatement au Groupe WEG tout manquement à la politique de sécurité de l'information pour les partenaires, par eux-mêmes ou par d'autres personnes, qu'elles soient ou non liées au partenaire.
- Respecter les conditions générales d'achat de biens, de matériels et/ou de services (« CCG ») du groupe WEG - disponibles à l'adresse : https://www.weg.net/ -> This is WEG -> GENERAL PURCHASING CONDITIONS FOR SUPPLIERS - et le code d'éthique du groupe WEG pour les fournisseurs (« code d'éthique ») - disponibles à l'adresse : https://www.weg.net/ -> This is WEG -> CODE D'ÉTHIQUE POUR LES FOURNISSEURS. Le partenaire doit se conformer strictement aux paramètres qui lui sont applicables en matière de protection des données et de la vie privée établis dans toute législation applicable, ainsi que suivre les meilleures pratiques du marché en la matière.
- Les partenaires qui exercent des activités critiques au nom du groupe WEG doivent se soumettre à un processus d'évaluation de la sécurité de l'information (SI). Dans le cadre du processus d'évaluation de la sécurité de l'information, une auto-évaluation de la sécurité de l'information sera effectuée au cours des phases de qualification du fournisseur et de négociation du contrat. En fonction du résultat de l'auto-évaluation, le groupe WEG peut demander des procédures supplémentaires pour vérifier l'adéquation du partenaire aux paramètres de sécurité de l'information établis dans la présente politique de sécurité de l'information pour les partenaires.

6. EXIGENCES EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

6.1. COMPORTEMENT DES PARTENAIRES DANS L'ENVIRONNEMENT DU GROUPE WEG

6.1.1. Accès logique et utilisation acceptable

- Pour les partenaires qui ont besoin d'accéder à l'environnement du Groupe WEG à distance, le gestionnaire WEG, responsable du contrat doit fournir l'accès par l'intermédiaire d'un utilisateur unique et individuel, dans lequel ils ne peuvent avoir accès qu'aux ressources et environnements de travail nécessaires à l'exercice de leurs fonctions ;

- Les ordinateurs des partenaires ne peuvent pas être connectés au réseau interne du Groupe WEG sans l'accord préalable du responsable de la sécurité de l'information, le logiciel de l'équipement des partenaires doit être dûment licencié ;
- Il est interdit d'accéder, de télécharger ou de distribuer tout contenu qui viole les droits d'auteur ou la propriété du Groupe WEG. De même, il est interdit d'accéder ou de distribuer des contenus illégaux, pornographiques de toute nature ou qui violent le statut de l'enfant et de l'adolescent ;
- Les identifiants d'accès mis à la disposition du partenaire sont à usage exclusif et ne peuvent être divulgués ou partagés avec d'autres ;
- Le partenaire doit conserver ses identifiants d'accès en toute sécurité, et il est seul et unique responsable de toute utilisation faite avec ses identifiants d'accès, y compris toute utilisation abusive;
- Il incombe au partenaire de communiquer tout licenciement de ses employés, fournisseurs ou prestataires de services.

6.1.2. Notification des incidents de sécurité de l'information

Lorsqu'il découvre un incident ou qu'il soupçonne raisonnablement qu'un incident se produit ou s'est produit, le partenaire doit:

- Il lance immédiatement le traitement de l'incident afin d'enquêter, de contenir rapidement et de protéger tous les systèmes informatiques et les données de l'entreprise en danger, de minimiser et d'atténuer l'impact de l'incident sur les systèmes informatiques ;
- Informer immédiatement le Groupe WEG par e-mail soc@weg.net.

Le partenaire doit notifier l'incident en fournissant les informations suivantes :

- La nature et la portée présumée de l'incident ;
- La date suspecte à laquelle l'incident a commencé ;
- La date et l'heure de la découverte de l'incident ;
- les mesures prises par le partenaire pour assurer la continuité de la fourniture du champ d'application et pour protéger et récupérer les données de l'entreprise, le cas échéant ; et
- les coordonnées d'un représentant du partenaire chargé de répondre aux demandes d'informations du groupe WEG.

Le partenaire doit fournir au groupe WEG les informations suivantes dès que possible :

- les causes présumées de l'incident et le(s) acteur(s) impliqué(s) ;
- L'impact estimé de l'incident ;
- les mesures correctives proposées et le délai estimé pour un rétablissement complet à la suite de l'impact de l'incident ;
- les mesures correctives proposées, notamment pour assurer la continuité de la fourniture du champ d'application et pour protéger et récupérer les données de l'entreprise, le cas échéant.

Le partenaire fournit au groupe WEG des mises à jour régulières des informations fournies conformément aux paragraphes précédents, ainsi que toute autre information que le groupe WEG peut raisonnablement demander en rapport avec l'incident (y compris les enregistrements de tous les accès aux systèmes informatiques pertinents en rapport avec l'incident et les preuves permettant de démontrer la protection et la récupération effectives des données de l'entreprise).

Le partenaire fournit immédiatement au groupe WEG toute l'assistance dont le groupe WEG peut avoir besoin pour lui permettre d'enquêter sur les incidents, d'y répondre, d'en atténuer l'impact et de les corriger (y compris la protection et la récupération des données de l'entreprise) et de communiquer et de répondre aux personnes ou aux autorités publiques, y compris les autorités de régulation compétentes.
Le partenaire fournit au groupe WEG un rapport final sur l'incident, y compris une analyse des causes profondes, dès que disponible.
Nonobstant toute disposition contraire au contrat, un incident n'est pas considéré comme un cas de force majeure dans la mesure où il est dû à une violation de la présente annexe ou à la négligence d'un membre du partenaire.

6.1.3. Sécurité des équipements

- Chaque partenaire est responsable de la protection des dispositifs physiques contenant des informations du Groupe WEG qui sont sous sa garde ; et
- Les partenaires sont conscients que l'accès à tout environnement du Groupe WEG ou l'utilisation de toute ressource informatique dans l'environnement du Groupe WEG, même dans les situations où le partenaire utilise un équipement qui lui appartient personnellement, sont soumis à une surveillance et à une inspection, sauf dans les situations où la loi locale applicable interdit expressément une telle conduite.

6.1.4. Violation de la politique de sécurité de l'information

Les situations suivantes sont considérées comme des violations de la présente politique de sécurité de l'information pour les partenaires, sans toutefois s'y limiter :

- Toute action, omission ou autre situation susceptible d'exposer le groupe WEG à une perte financière ou d'image, directe ou indirecte, potentielle ou réelle, compromettant ses actifs informationnels
- l'utilisation abusive ou la divulgation de toute information sans l'autorisation expresse du groupe WEG, telle que des données d'entreprise, des secrets commerciaux ou d'autres informations ;
- Le non-respect, commis ou omis, d'une ligne directrice, d'une règle, d'un paramètre ou d'une obligation établis dans la présente politique de sécurité de l'information à l'intention des partenaires ;
- l'utilisation de données, d'informations, d'équipements, de logiciels, de systèmes ou d'autres ressources technologiques à des fins illicites, ce qui peut inclure la violation des lois, des réglementations internes et externes, de l'éthique ou des exigences des organismes de réglementation dans le domaine d'activité du Groupe WEG ; et
- le fait de ne pas communiquer immédiatement au groupe WEG tout incident lié à la sécurité de l'information ou le non-respect de la présente politique de sécurité de l'information pour les partenaires.

6.2. CONTRÔLES DE SÉCURITÉ ET DE CONFIDENTIALITÉ DANS L'ENVIRONNEMENT DU PARTENAIRE

À la demande du secteur d'activité du groupe WEG, le partenaire en question sera enregistré par l'équipe de gouvernance de la sécurité de l'information dans un outil destiné à vérifier sa cybersanté. Cette plateforme fournit des scores.
Le score global du partenaire doit atteindre au moins 80 % ou le score moyen de son segment de marché fourni par l'outil lui-même, le plus élevé des deux étant retenu.

Les partenaires qui n'atteignent pas le score souhaité recevront un rapport d'adéquation et de conformité du groupe WEG afin que le partenaire puisse prendre des mesures pour atteindre le score souhaité dans un délai de 180 jours.
Outre la procédure d'enregistrement décrite ci-dessus, le partenaire doit suivre les lignes directrices suivantes en matière de sécurité de l'information, également prévues dans le document d'auto-évaluation envoyé et tenu à jour par le secteur de la sécurité de l'information.

6.2.1. Protection de la vie privée

- Présenter, à l'aide de documents, le flux des données WEG dans l'environnement du partenaire, en décrivant l'ensemble de leur cycle de vie (collecte, traitement, stockage, partage et suppression).
- Informer le Groupe du WEG des informations collectées, de leur finalité, de la base juridique du traitement des données, de l'endroit où elles sont stockées et de leur durée, en cherchant toujours à réduire au minimum la période de stockage et la quantité d'informations collectées.
- Disposer d'une analyse d'impact relative aux données personnelles d'un détenteur (DPIA), ainsi que d'un processus permettant au groupe WEG d'accéder sans restriction aux informations traitées et stockées, conformément au champ d'application du contrat.
- Disposer d'une procédure d'acceptation et de refus permettant au groupe WEG et aux détenteurs de données personnelles de s'exprimer librement et au préalable sur le partage des données dans le cadre d'un partenariat. Il convient également de noter que la valeur par défaut doit être le non-partage. Ce n'est qu'après avoir obtenu l'accord de la partie intéressée que le partenaire pourra partager des données avec des partenaires.

6.2.2. Contrôle de la réussite

- disposer d'un processus de gestion de l'accès correctement documenté ;
- donner au groupe WEG un accès illimité aux données et aux informations stockées ou à traiter, conformément aux services spécifiques définis, en valorisant la confidentialité, l'intégrité, la disponibilité et la capacité de récupération de ces données et informations
- Donner au groupe WEG une visibilité sur les procédures et les contrôles utilisés pour respecter le contrat, comme décrit au point ci-dessus, en particulier pour l'identification et la séparation des données des clients du groupe WEG, par le biais de contrôles physiques ou logiques ;
- Ne pas autoriser l'utilisation de comptes partagés ou d'utilisateurs génériques pour les systèmes critiques, et maintenir des contrôles liés à la connexion, tels que (mais sans s'y limiter) : forcer les changements lors du premier accès, bloquer l'utilisateur après un certain nombre de tentatives non valides, exiger des modèles de mots de passe complexes et d'autres pratiques de sécurité de l'information conformes aux meilleures normes du marché ;
- Disposer d'un processus formalisé et documenté pour l'octroi, la modification et la révocation de l'accès, en particulier pour les personnes bénéficiant d'actions privilégiées ;
- Disposer d'un processus de contrôle de l'absence de séparation des fonctions (SOD) ;
- Adopter une politique de moindre privilège ;
- Disposer de méthodes de contrôle d'accès physique et logique des visiteurs ; et

- Disposer de contrôles d'accès à distance pour les employés/fournisseurs de services pendant les périodes de *télétravail.*

6.2.3. Contrôle des services et gestion des opérations de sécurité de l'information

- Veiller à ce qu'il dispose du plus haut niveau de capacité pour fournir des informations et des ressources de gestion adéquates pour contrôler les services à fournir, ainsi que pour assurer le respect de la législation et de la réglementation en vigueur ;
- Informer le Groupe WEG et lui donner accès, sur demande, aux ressources de gestion appropriées pour le suivi des services contractuels ;
- Disposer de ressources et d'outils pour surveiller la capacité et la disponibilité de vos actifs, corréler les alertes et générer des tickets d'incident de manière automatisée ;
- Disposer d'un processus structuré de réponse aux incidents, y compris la catégorisation des incidents et les manuels d'exécution pour le traitement et la résolution des incidents connus.
- Prévenir, détecter et réduire les incidents liés à l'environnement cybernétique, en justifiant de procédures et de contrôles qui couvrent, au minimum, l'authentification, le cryptage, la prévention et la détection des intrusions, la prévention des fuites de données, les tests et analyses périodiques pour détecter les vulnérabilités, l'application de correctifs de sécurité, l'application de durcissements sur ses serveurs et postes de travail, la protection contre les logiciels malveillants et le blocage des logiciels non approuvés, la mise en place de mécanismes de traçabilité et de segmentation du réseau informatique, la maintenance des copies de sécurité des données et de l'information ;
- WEG se réserve le droit de révoquer immédiatement et unilatéralement tout accès en cas d'incident de sécurité ou de comportement anormal/inapproprié dans l'environnement WEG impliquant le partenaire, qu'il soit confirmé, soupçonné ou fasse l'objet d'une enquête ;
- Fournir, sur demande, des informations relatives au nombre d'incidents survenus au cours des 24 derniers mois, en les classant en fonction de leur pertinence. Toutes les données relatives aux incidents de gravité « moyenne », « élevée » ou « très élevée » doivent être conservées par le partenaire pendant au moins cinq ans ; et
- Tenir le Groupe WEG informé en permanence de toute limitation susceptible d'affecter la fourniture des services ou le respect de la législation et de la réglementation en vigueur.

6.2.4. Gestion des menaces

Le partenaire veille à ce que les vulnérabilités des systèmes informatiques soient corrigées ou mises à jour en temps utile. En tout état de cause, le partenaire doit

a) Dans les 24 heures suivant la découverte d'une vulnérabilité critique (CVSS ou CVE 9.0 ou plus) dans les systèmes informatiques concernés du groupe contractant qui n'est pas fournie par un tiers :

- Commencer le processus de développement et de déploiement d'une mise à jour ou d'un correctif pour corriger la vulnérabilité ;
- Notifier le Groupe WEG à l'adresse soc@weg.net et fournir des détails sur la vulnérabilité et la menace associée, ainsi que sur les mesures mises en œuvre par le partenaire pour atténuer la menace ou la vulnérabilité.
- Veiller à ce que tous les systèmes informatiques pertinents du partenaire soient dotés des derniers correctifs fournis par des tiers et installés et déployés ; et

- Installer et déployer les mises à jour ou les correctifs pour les vulnérabilités figurant dans le catalogue des vulnérabilités exploitées connues de la U.S. Cyber & Infrastructure Security Agency dans les 24 heures suivant la publication de la mise à jour ou du correctif. Si une mise à jour ou un correctif ne peut être appliqué pour une raison quelconque dans les 24 heures, le partenaire doit en informer immédiatement le Groupe WEG à l'adresse soc@weg.net.

b) Le partenaire doit :

- Veiller à ce que les systèmes informatiques pertinents soient contrôlés en permanence afin de garantir leur sécurité, leur authenticité, leur confidentialité, leur intégrité et leur disponibilité ; et
- Générer en permanence les journaux des systèmes informatiques pertinents nécessaires pour : (A) permettre la réponse aux incidents ; (B) identifier la source d'un incident ; et (C) recréer la séquence des événements ayant conduit à un incident. Le partenaire doit conserver ces enregistrements en toute sécurité pendant au moins 180 jours à compter de la date de leur création, de manière à ce que seuls les utilisateurs autorisés puissent y accéder.

6.2.5. La sécurité dans le développement de systèmes

- Adoptez des pratiques de protection de la vie privée et de sécurité dès la conception dans vos processus de développement de logiciels ;
- Décrire les caractéristiques de sécurité et les données auxquelles accèdent les applications, qui doivent être évaluées par le service de sécurité de l'information au cours de la phase d'approbation (ex : spécification technique et/ou diagramme fonctionnel) ;
- Utiliser des routines de validation de l'intégrité pour éviter les erreurs, qu'elles soient involontaires ou intentionnelles, en utilisant des données fictives ou des anonymisations dans un environnement non productif ;
- Adopter des pratiques d'analyse de la sécurité dans le code source ;
- Adopter des pratiques d'analyse de la sécurité dans leurs applications (tests de piratage éthique et tests de pénétration) ;
- Prévoir des validations de sécurité dans le processus de qualité et de vérification du code. Au minimum, ceux qui figurent dans le TOP 10 de l'OWASP devraient être pris en considération.

6.2.6. Continuité des activités, gestion, conservation et stockage des données.

- Définir un programme de continuité des activités pour garantir que d'éventuels incidents n'affectent pas les services fournis au Groupe WEG, en envisageant en particulier le plan de reprise après sinistre, en testant régulièrement les contrôles d'assurance afin de vérifier dans quelle mesure l'entreprise est préparée à des cas réels ;
- Informer le Groupe WEG et lui donner accès, sur demande, aux mesures de sécurité concernant la transmission et le stockage des données et des informations, ainsi que leur élimination, en utilisant des procédures d'exclusion sécurisées (numériques et/ou physiques) ;
- Disposer d'un processus de sauvegarde exécuté périodiquement sur les actifs qui stockent les informations du Groupe WEG, afin d'éviter ou de minimiser la perte de données en cas d'incident.

6.2.7. Formation et sensibilisation

- Garantir l'existence d'un programme de formation et de sensibilisation à la sécurité de l'information et à la confidentialité des données, avec une périodicité minimale annuelle, pour tous ses employés, fournisseurs et prestataires de services, et la formation doit être envisagée avec l'application obligatoire du code de conduite des partenaires pour les employés, fournisseurs et prestataires de services nouvellement embauchés.
- Inclure dans son programme de formation et de sensibilisation à la sécurité de l'information et à la confidentialité des données des campagnes de prévention de l'hameçonnage et des conseils sur l'ingénierie sociale, ainsi que des conférences, la publication de bulletins d'information sur la sécurité de l'information et la confidentialité des données, etc.
- Les employés, fournisseurs et prestataires de services des partenaires qui ont accès à des données à caractère personnel et/ou à des informations sensibles ou qui les traitent doivent avoir connaissance de la présente politique et de ce qu'elle implique en matière de formation à la sécurité de l'information.

6.2.8. Services et certifications

Le partenaire doit :

- Notifier, à l'avance et de manière formelle, la sous-traitance de services en rapport avec l'objet du contrat avec le Groupe WEG ;
- Disposer de reconnaissances en matière de sécurité de l'information ou de continuité des activités, prouvées par des rapports d'audit externes indépendants ;
- Informer le Groupe WEG et lui donner accès, sur demande, aux certifications nécessaires à la fourniture des services, ainsi qu'aux rapports relatifs aux contrôles utilisés dans la fourniture des services contractuels, préparés par un cabinet d'audit indépendant spécialisé ; et
- Disposer de mécanismes permettant de communiquer les anomalies ou les incidents de sécurité au groupe WEG, aux personnes concernées et à l'autorité nationale de protection des données.

7. ÉVALUATIONS PÉRIODIQUES

Le Groupe WEG peut procéder, chaque fois qu'il le juge nécessaire, à des évaluations pour attester de l'efficacité de la mise en œuvre des contrôles présentés dans le présent document et, à cette fin, il doit en informer le partenaire 30 jours à l'avance. Des évaluations peuvent également avoir lieu en cas d'incident de sécurité ou de changement des conditions de marché applicables au segment du partenaire ou du Groupe WEG.

8. SANCTIONS

La violation d'un contrôle ou le non-respect de la politique de sécurité de l'information pour les partenaires et de ses définitions sont considérés comme des fautes ou des violations graves, et les pénalités ou sanctions applicables peuvent être appliquées conformément aux politiques internes du groupe WEG et/ou prévues dans le contrat.

En cas de violation de toute obligation ou disposition de la présente politique par le partenaire, ses employés, fournisseurs, prestataires de services et/ou toute personne liée au partenaire, le partenaire s'engage à indemniser, à dégager de toute responsabilité, à défendre et à dégager le groupe WEG de toute perte ou dommage, sans préjudice d'autres pénalités, sanctions et/ou peines prévues dans le contrat ou par la loi.

Le partenaire reconnaît et accepte que la simple indemnisation peut ne pas être le moyen approprié de remédier à toute violation de la présente politique, et que le groupe WEG peut utiliser toute forme et/ou moyen d'exécution spécifique des obligations qui peuvent être applicables en cas de menace de violation ou de violation effective du présent partenariat.