**Mesures de sécurité**

| | |
|---|---|
| **Présentées par :** | **ADP - Organisation de la sécurité mondiale** |
| **Version :** | **2.0** |
| **Publication :** | **Septembre 2019** |

**Table des matières**

**Termes et définitions**

Les termes suivants apparaissent tout au long du document :

| Terme ou acronyme utilisé | Définition |
|---|---|
| GETS | « Global Enterprise Technology & Solutions » (Technologie et Solutions de l'Organisation Mondiale) |
| GSO | « Global Security Organization » (Organisation de la sécurité mondiale) |
| CAB | « Change Advisory Board » (Comité consultatif sur les changements) |
| DRP | « Disaster Recovery Plan » (Plan de reprise après sinistre) |
| CIRC | « GSO's Critical Incident Response Center » (Centre d'intervention en cas d'incident critique) du « GSO » |
| SIEM | « Security Information and Event Management » (Sécurité des informations et gestion des événements) |
| IDS | « Intrusion Detection System » (Système de détection des intrusions) |
| DNS | « Domain Name System » (Systèmes de noms de domaines) |
| NTP | « Network Time Protocol » (Protocole de temps réseau) |
| SOC | « Service Organization Controls » (Contrôles de l'organisation des services) |
| TPSI | « Trusted Platform Security Infrastructure » (Infrastructure de sécurité des plateformes de confiance) |


| Terme ou acronyme utilisé | Définition |
|---|---|
| GETS | « Global Enterprise Technology & Solutions » (Technologie et Solutions de l'Organisation Mondiale) |

**Vue d'ensemble**

ADP dispose d'un programme de sécurité de l'information officiel qui contient des mesures de protection physiques, techniques et administratives destinées à préserver la sécurité, la confidentialité et l'intégrité des informations des clients. Ce programme est raisonnablement destiné à (i) protéger la sécurité et la confidentialité des informations des clients (ii) protéger contre les risques ou les menaces pesant sur la sécurité ou l'intégrité des informations, et (iii) protéger contre des accès aux informations ou une utilisation de celles-ci non autorisés.

Ce document contient une vue d'ensemble des mesures et des pratiques destinées à assurer la sécurité des informations d'ADP à la date de publication et susceptibles d'être modifiées par ADP. Ces exigences et pratiques sont conçues pour être conformes aux normes de sécurité de l'information ISO/IEC 27001:2013. ADP évalue régulièrement ses politiques et normes relatives à la sécurité. Notre but est d'aider à garantir que le programme de sécurité fonctionne de manière efficace et économique pour protéger toutes les informations que nos clients et leurs employés nous confient.

## Section 1 - Politique de sécurité de l'information

### Indépendance de la fonction de sécurité de l'information

Le chef de la sécurité d'ADP supervise l'Organisation de la sécurité mondiale (GSO) d'ADP et rend compte à l'Avocat général plutôt qu'au chef des services de l'information, ce qui confère à GSO l'indépendance nécessaire par rapport au service informatique. GSO est une équipe de sécurité centralisée inter-divisions qui adopte une approche multidisciplinaire en matière de conformité aux normes de sécurité de l'information et cybernétique, et de gestion du risque opérationnel, gestion de la sécurité des clients, protection de la main d'œuvre et résilience d'entreprise. Les responsables du GSO, sous la direction de notre chef de la sécurité, sont chargés de la gestion des politiques, procédures et directives relatives à la sécurité.

### Définition officielle d'une politique de sécurité de l'information

ADP a élaboré et documenté des politiques de sécurité de l'information officielles qui définissent l'approche d'ADP en matière de gestion de la sécurité de l'information. Les domaines spécifiques couverts par cette politique comprennent, sans s'y limiter :

- **Politique de gestion de la sécurité** - présente les responsabilités de l'Organisation de la sécurité mondiale (GSO) et du chef de la sécurité (CSO), y compris les responsabilités en matière de sécurité de l'information et les contrôles sur le processus d'embauche du point de vue de la sécurité.
- **Politique de confidentialité mondiale** - décrit la collecte de données personnelles, l'accès à ces dernières, leur exactitude, leur divulgation et les politiques de confidentialité relatives aux clients.
- **Politique des employés sur l'utilisation acceptable des communications électroniques et la protection des données** - décrit l'utilisation acceptable des différentes communications électroniques, du cryptage et de la gestion des clés.
- **Politique sur le traitement de l'information** - présente les exigences relatives à la classification des informations d'ADP et établit des contrôles permettant la protection de ces dernières.
- **Politique relative à la sécurité physique** - définit les exigences de sécurité des installations d'ADP et donc celles applicables aux visiteurs et aux employés qui y travaillent.
- **Politique de gestion des opérations de sécurité** - indique les contrôles minimaux pour maintenir les correctifs du système, traiter efficacement la menace des logiciels malveillants et contrôler la sécurité des sauvegardes et des bases de données.
- **Politique de surveillance de la sécurité** - fournit des contrôles pour les systèmes de détection d'intrusion, les journaux et la prévention des pertes de données.
- **Politique sur les enquêtes et la gestion des incidents** - définit des normes pour la réponse aux incidents, la découverte électronique, la protection de la main-d'œuvre, et l'accès aux données électroniques stockées des employés.
- **Politique sur l'accès et l'authentification** - présente les exigences en matière d'authentification (par exemple, nom d'utilisateur et mot de passe), d'accès à distance et d'accès sans fil.
- **Politique de sécurité réseau** - architecture de sécurité des routeurs, pare-feu, AD, DNS, serveurs de messagerie, DMZ, services infonuagiques, périphériques réseau, proxy Web et technologie de réseau commuté.
- **Politique d'assurance des vendeurs** - définit les contrôles minimaux de sécurité pour qu'une tierce partie puisse aider ADP à atteindre ses objectifs commerciaux.
- **Politique de gestion des applications -** établit des contrôles de sécurité appropriés à chaque étape du cycle de vie de développement du système.

- **Politique de résilience des activités** - régit la protection, l'intégrité et la préservation d'ADP en établissant les exigences minimales pour documenter, mettre en œuvre, maintenir et améliorer continuellement les programmes de résilience des activités.
- **Politique de gestion des risques centralisés -** identification, surveillance, réponse, analyse, gouvernance et nouvelles initiatives commerciales.

Ces politiques sont publiées sur le site intranet d'ADP et sont accessibles par tous les employés et entrepreneurs au sein du réseau d'ADP.

**Examen de la Politique de sécurité de l'information**

ADP examine ses politiques de sécurité de l'information au moins une fois par an ou lors de tout changement majeur ayant un impact sur le fonctionnement des systèmes d'information d'ADP.

## Section 2 - Organisation de la sécurité de l'information

### Rôles et responsabilités dans le domaine de la sécurité de l'information

Le GSO regroupe des équipes de sécurité inter-divisions s'appuyant sur une approche multidisciplinaire en matière de conformité aux normes de sécurité de l'information et cybernétique, et de gestion du risque opérationnel, gestion de la sécurité des clients, protection de la main d'œuvre et résilience d'entreprise. Ses rôles et responsabilités ont été officiellement définis par tous les membres du GSO. Le GSO est chargé de la conception, de la mise en œuvre et de la surveillance de notre programme de sécurité de l'information fondé sur les politiques de l'entreprise. Les activités du GSO sont supervisées par le Comité de direction sécurité, composé du chef de la sécurité, le directeur général, le directeur financier, le directeur de la stratégie, le directeur des ressources humaines et le directeur juridique d'ADP.

### Informatique mobile et politique de télétravail

ADP exige le cryptage de toutes les informations confidentielles sur les appareils mobiles pour éviter les fuites de données qui pourraient résulter du vol ou de la perte d'un ordinateur ou d'un appareil. Une protection avancée des terminaux et l'authentification à deux facteurs sur VPN sont également nécessaires pour accéder à distance aux réseaux de l'entreprise. Tous les appareils à distance doivent être protégés par un mot de passe. Les employés d'ADP doivent signaler toute perte ou tout vol d'appareil informatique distant à l'aide d'un processus de déclaration d'incident de sécurité.

Tous les employés et entrepreneurs, doivent respecter, et c'est une condition de leur emploi par ADP, la politique sur l'utilisation acceptable des communications électroniques et la protection des données et d'autres politiques pertinentes.

## Section 3 - Sécurité des ressources humaines

### Vérifications des antécédents

Conformément aux exigences légales applicables dans le pays de la personne, ADP réalise des vérifications des antécédents correspondant aux fonctions et aux responsabilités de ses employés, entrepreneurs et des tierces parties. Ces vérifications visent à confirmer qu'un candidat devant traiter des données de clients convient avant son engagement ou son embauche.

Ces vérifications d'antécédents peuvent comprendre les éléments suivants :

- Vérification de l'identité/de l'employabilité
- Expérience professionnelle
- Antécédents de formation et de qualification professionnelle
- Casier judiciaire (lorsque c'est légal et en fonction des réglementations nationales locales)

### Accords de confidentialité avec les employés et entrepreneurs

Les contrats de travail d'ADP et les contrats avec des entrepreneurs contiennent des conditions qui indiquent les obligations et les responsabilités liées aux données des clients auxquelles ils ont accès. Tous les employés et les entrepreneurs d'ADP doivent respecter des obligations de confidentialité.

### Programme de formation à la sécurité des données

Tous les employés doivent participer à une formation à la sécurité des données dans le cadre de leur plan d'intégration. De plus, ADP offre une formation à la sécurité annuelle pour rappeler aux employés leurs responsabilités dans l'exercice de leurs fonctions.

### Responsabilités des employés et procédures disciplinaires

ADP a publié une politique de sécurité que tous les employés doivent respecter. Les infractions aux politiques de sécurité peuvent conduire à une révocation des privilèges d'accès et/ou des mesures disciplinaires pouvant aller jusqu'à la résiliation des contrats de conseil ou le licenciement.

### Responsabilités lors d'une cessation d'emploi

Les responsabilités lors d'une cessation d'emploi ont été officiellement documentées et incluent, au minimum :

- Le retour de tous les actifs et toutes les données d'ADP en possession de l'employé concerné, quel que soit le support de stockage
- La résiliation des droits d'accès aux installations, aux données et aux systèmes d'ADP
- Le changement des mots de passe pour les comptes partagés actifs restants, le cas échéant
- Le transfert des connaissances, le cas échéant.

## Section 4 - Gestion d'actifs

### Utilisation acceptable des actifs

L'utilisation acceptable des actifs est expliquée dans plusieurs politiques applicables aux employés d'ADP et aux entrepreneurs, afin de s'assurer que les données d'ADP et des clients ne sont pas exposées à des risques liés à l'utilisation de ces actifs. Des exemples des domaines décrits dans ces politiques sont : l'utilisation de communications électroniques, l'utilisation des équipements électroniques et l'utilisation des actifs informationnels.

### Classification des données

Les données acquises, créées ou conservées par ou pour le compte d'ADP se voient attribuer, selon le cas, les classifications de sécurité suivantes :

- Publique - Exemple : brochures commerciales, rapports annuels publiés
- À usage interne d'ADP uniquement - Exemple : communications interbureaux, procédures opérationnelles
- Confidentielles ADP - Exemple : données personnelles et données personnelles de nature délicate
- Restreintes ADP - Exemple : prévisions financières, informations de planification stratégique

Les exigences en matière de traitement des données sont directement corrélées à la classification de sécurité des données. Les données personnelles et les données personnelles de nature délicate sont toujours considérées comme confidentielles ADP. Toutes les données des clients sont classifiées comme confidentielles.

Les employés d'ADP sont responsables de la protection et du traitement des actifs informationnels conformément à leur niveau de classification de sécurité, qui prévoit les exigences de protection de l'information et de traitement applicables pour chaque niveau de classification. La classification de confidentialité d'ADP est appliquée à toutes les données stockées, transmises et traitées par des tiers.

### Élimination des équipements et des supports

Lorsque des équipements, documents, fichiers et supports sont éliminés ou réutilisés, des mesures appropriées sont prises pour éviter une récupération future des données des clients qui y étaient initialement stockées. Toutes les données sur des ordinateurs ou des supports de stockage électroniques, quelle que soit leur classification, sont éliminées de manière sécurisée, sauf lorsque le support est détruit physiquement avant de quitter les installations d'ADP ou d'être recyclé. Les procédures de destruction sécurisée/d'effacement des données d'ADP contenues dans des équipements, documents, fichiers et supports sont documentées officiellement.

### Supports physiques en transit

Des protections organisationnelles ont été mises en œuvre pour protéger les supports écrits contenant des données des clients contre le vol, la perte ou un accès ou une modification non autorisés (i) lors de leur transport, par exemple des enveloppes scellées, des contenants et des livraisons en main propre aux utilisateurs autorisés; et (ii) au cours de l'examen, de la révision ou d'autres traitements hors du lieu de stockage sécurisé.

## Section 5 - Contrôle des accès

### Exigences commerciales de contrôle des accès

La politique de contrôle de l'accès d'ADP est fondée sur des exigences définies par l'entreprise. Les politiques et les normes de contrôle sont organisées autour de contrôles d'accès qui sont appliqués obligatoirement dans tous les composants du service fourni et sont fondés sur des principes du « moindre privilège » et du « besoin de savoir ».

### Accès aux infrastructures - Gestion du contrôle des accès

Les demandes d'accès pour déplacer, ajouter, créer et effacer des données sont enregistrées, approuvées et revues régulièrement.

Un examen officiel est effectué au moins une fois par an pour confirmer que chaque utilisateur a accès à l'activité opérationnelle pertinente et n'a plus le même accès après un changement d'activité. Ce processus est vérifié et documenté dans un rapport de type II SOC1[1]. Au sein du système de gestion des identités, une équipe ADP dédiée est responsable de l'octroi, du refus, de l'annulation, de la résiliation et du démantèlement/de la désactivation des accès aux installations et aux systèmes d'information d'ADP. ADP utilise un outil de gestion des identités et des accès (GIA) centralisé qui est géré centralement par une équipe de GETS dédiée. Selon la demande de droit d'accès effectuée par l'intermédiaire de l'outil de GIA, un flux de travail de validation est déclenché pouvant impliquer le responsable de l'utilisateur. Les accès sont accordés temporairement et il existe des flux de travail pour éviter que de tels accès restent permanents. L'accès d'un employé à une installation est annulé immédiatement après son dernier jour d'emploi en désactivant sa carte d'accès (le badge de l'employé). Les identifiants d'utilisateur des employés sont désactivés immédiatement. Tous les actifs des employés sont retournés et vérifiés par le responsable hiérarchique compétent et sont comparés par rapport à la liste d'actifs dans la base de données de gestion des configurations. Suite à un changement de poste ou organisationnel, les profils ou les droits d'accès des utilisateurs doivent être modifiés par les équipes de gestion de l'unité fonctionnelle et de GIA. De plus, un examen officiel des droits d'accès a lieu chaque année pour vérifier que les droits de chaque utilisateur correspondent bien à leur activité et qu'il ne reste pas de droits d'accès non pertinent après un changement de poste.

### Politique de mot de passe

Les politiques de mot de passe des employés d'ADP sont appliquées obligatoirement dans les appareils et applications des serveurs, bases de données et réseaux, dans la mesure permise par l'appareil/l'application. La complexité du mot de passe est fonction d'une analyse fondée sur les risques des données et du contenu protégés. Les politiques respectent les normes du secteur en matière de robustesse et de complexité, y compris sans s'y limiter, l'utilisation d'une authentification progressive, à deux facteurs ou biométrique le cas échéant.

Les exigences d'authentification d'une application client varient par produit, et des services fédérés (SAML 2.0) sont disponibles sur des applications ADP spécifiques utilisant un réseau unifié et une couche de sécurité gérée par GETS.

[1] Dans le cas de certains services américains offerts par ADP, cela fait l'objet d'une vérification dans un rapport de type 2 SOC2.

**Expiration des sessions**

ADP applique une expiration automatique des connexions de tous les serveurs, postes de travail, applications et VPN selon une approche fondée sur les risques conforme aux normes du secteur. Le rétablissement de la connexion ne peut avoir lieu qu'après la saisie d'un mot de passe valide par l'utilisateur.

## Section 6 - Cryptographie

### Contrôles cryptographiques

ADP exige que les informations sensibles échangées entre ADP et des tiers soient cryptées (ou que le canal de transmission soit lui-même crypté) selon une robustesse et à l'aide de techniques de cryptage acceptées par le secteur. Sinon, une ligne louée privée doit être utilisée.

### Gestion des clés

ADP a mis en place une norme de sécurité du cryptage interne qui inclut des procédures de gestion et de récupération des clés, notamment une gestion des clés à la fois symétrique et asymétrique.

Les clés de cryptage utilisées pour les données d'ADP sont toujours classées comme des informations confidentielles. L'accès à ces clés est strictement limité à ceux qui « ont besoin de savoir » et si une approbation d'exception est accordée. Les clés de cryptage et la gestion du cycle de vie des clés respectent les pratiques courantes du secteur.

## Section 7 - Sécurité physique et environnementale

L'approche d'ADP en matière de sécurité physique a deux objectifs : créer un environnement de travail sûr pour les collaborateurs d'ADP et protéger les données personnelles détenues dans les centres de données d'ADP et les autres emplacements stratégiques d'ADP.

La politique de sécurité d'ADP oblige ses responsables à identifier les zones nécessitant un niveau spécifique de sécurité physique. L'accès à ces zones n'est accordé qu'aux collaborateurs habilités à des fins autorisées. Les zones sécurisées d'ADP utilisent divers dispositifs de sécurité physique, notamment des systèmes de vidéo surveillance, l'utilisation de badges de sécurité (accès contrôlés en fonction de l'identité) et des agents de sécurité postés aux points d'entrée et de sortie. Les visiteurs ne peuvent se voir accorder l'accès que sur autorisation et sont surveillés en permanence.

## Section 8 - Sécurité des opérations

### Formalisation des procédures opérationnelles du service informatique.

GETS est l'unité d'ADP responsable du fonctionnement et de la maintenance de l'infrastructure informatique. GETS documente et met à jour officiellement les politiques et procédures informatiques. Ces procédures comprennent, sans s'y limiter :

- La gestion du changement
- La gestion des sauvegardes
- Le traitement des erreurs système
- Le redémarrage et la restauration des systèmes
- La surveillance des systèmes
- La planification et la surveillance des tâches

### Gestion du changement des infrastructures

Un comité consultatif sur le changement (CCC) périodique, qui inclut des représentants de nombreuses équipes d'ADP, est réuni par GETS. Les réunions du CCC discutent de l'impact des fenêtres de déploiement et des mises en production, et permettent de coordonner tout autre changement de l'infrastructure de production.

### Planification et acceptation des capacités des systèmes

Les exigences de capacité sont surveillées en permanences et revues régulièrement. Après ces revues, les tailles des systèmes et des réseaux sont augmentées et réduites en conséquence. Lorsque des changements importants doivent être effectués en raison d'un changement de capacité ou de l'évolution d'une technologie, l'équipe d'étalonnage de GETS peut réaliser des tests de résistance sur les applications et/ou systèmes concernés. À la fin des tests de résistance, l'équipe fournit un rapport détaillé de l'évaluation de la performance en évaluant les changements dans (i) les composants (ii) la configuration ou la version du système ou (iii) la configuration ou la version de l'intergiciel.

### Protection contre les programmes malveillants

Des technologies de protection des terminaux aux normes du secteur sont utilisées pour protéger les actifs d'ADP conformément aux meilleures pratiques du secteur.

### Politique de gestion des sauvegardes

ADP a mis en place des politiques qui exigent de toutes les opérations d'hébergement de la production de sauvegarder les données de production. La portée et la fréquence des sauvegardes correspondent aux exigences commerciales des services d'ADP concernés, aux exigences de sécurité des données en question et au caractère critique des données dans le cadre d'une reprise après sinistre. La surveillance des sauvegardes programmées est effectuée par GETS, afin d'identifier les problèmes de sauvegarde ou les exceptions y relatives.

### Connexion de sécurité et surveillance

ADP a mis en place une infrastructure de connexion centrale et en lecture seule (SIEM) et un système de corrélation des connexions et d'alerte (TPSI). Les alertes de connexion sont surveillées et traitées rapidement par le CIRC.

Tous ces systèmes sont synchronisés à l'aide d'un Network Time Protocol (NTP) unique à référence d'horloge.

Chaque connexion contient au minimum :

- L'horodatage
- L'identité (de l'opérateur ou de l'administrateur)
- L'objet (information concernant l'événement)

Les pistes de vérification et les connexions au système pour les applications d'ADP sont conçues et établies pour enregistrer les informations suivantes :

- Les accès autorisés
- Les opérations privilégiées
- Les tentatives d'accès non autorisés
- Les alertes ou défaillances du système
- Les modifications des paramètres de sécurité du système, lorsque celui-ci permet un tel enregistrement

Seul le personnel autorisé d'ADP a accès à ces enregistrements, qui sont envoyés en direct pour éviter que les données soient falsifiées avant d'être stockées dans les dispositifs d'enregistrement sécurisés.

**Systèmes et surveillance des infrastructures**

ADP prend les mesures appropriées pour surveiller les infrastructures 24 heures sur 24 et 7 jours sur 7. Les alertes de perturbation sont gérées par différentes équipes en fonction de leur sévérité et des compétences requises pour résoudre le problème.

Les installations de centre d'hébergement d'ADP utilisent des applications de surveillance qui fonctionnent en permanence sur tous les systèmes de traitement connexes et sur les composants du réseau pour fournir au personnel d'ADP des avis proactifs sur les problèmes et des avertissements avant des problèmes éventuels.

**Gestion de la vulnérabilité technique**

Un système d'exploitation à la sécurité renforcée (ou un processus sécurisé) doit être installé sur tous les ordinateurs faisant partie de l'infrastructure d'hébergement. Les opérations hébergées emploient une version renforcée, approuvée et standardisée pour tous les types de serveurs utilisés au sein de nos infrastructures. Les installations standard des systèmes d'exploitation sont interdites, puisque de telles installations pourraient créer des vulnérabilités, comme des mots de passe de compte système génériques, qui introduiraient un risque d'infrastructure. Ces configurations réduisent le risque que des ordinateurs hébergés fassent tourner des services inutiles qui pourraient créer des vulnérabilités.

ADP a documenté une méthodologie pour les mises à jour, des évaluations de vulnérabilité régulières et des examens de la conformité des applications connectées à Internet et de leurs composants matériels correspondants, qui incluent au moins 15 catégories de tests principales. La méthode d'évaluation est fondée sur les meilleures pratiques internes et du secteur, notamment celles de l'Open Web Application Security Project (OWASP), du SANS Institute et du Web Application Security Consortium (WASC).

## Section 9 - Sécurité des communications

### Gestion de la sécurité du réseau

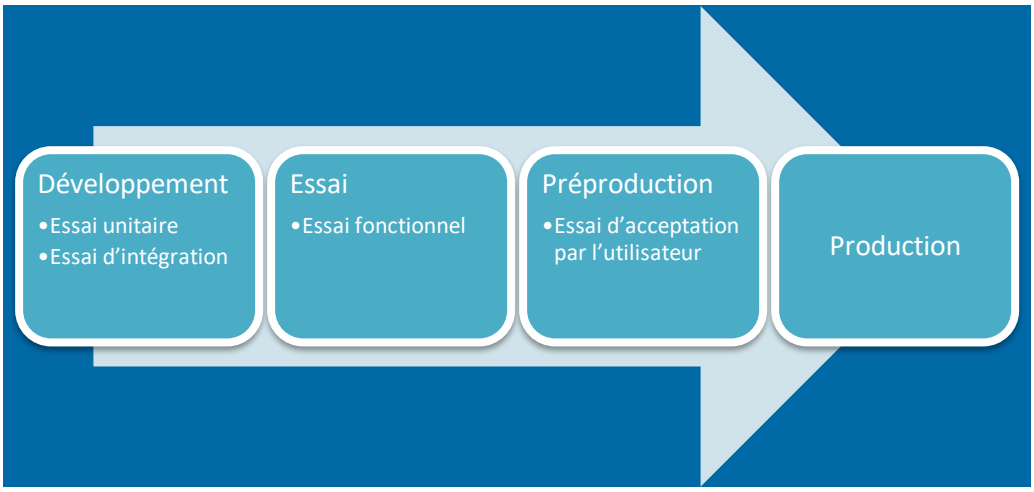
ADP emploie un système de détection des intrusions fondé sur le réseau qui surveille le trafic au niveau de l'infrastructure réseau (24 heures sur 27, 7 jours sur 7) et identifie les activités suspectes ou les attaques potentielles.

### Échange d'informations

ADP met en œuvre des contrôles appropriés de sorte que les données des clients d'ADP envoyées à des tiers soient transférées entre des systèmes et ressources informatiques autorisés seulement, et soient échangées uniquement à l'aide des mécanismes de transfert autorisés et sécurisés d'ADP.

### Sécurité lors du développement et processus de soutien

Au cours du cycle de développement, la documentation appropriée est produite, et des plans de test sont élaborés pour la phase de tests. Différentes étapes sont définies pour chaque environnement, chacune d'elle devant recevoir l'approbation appropriée :




- Pour passer de l'environnement de test à celui de pré-production, il faut l'approbation de l'équipe qualité d'ADP.
- Pour passer de l'environnement de pré-production à celui de production, il faut l'approbation des opérations informatiques.

Les équipes de développement doivent utiliser des méthodes de programmation sécurisées. Les changements d'application sont testés dans des environnements de développement et de régression avant d'atteindre les systèmes de production. Des tests sont réalisés et documentés. Une fois approuvés, les changements sont déployés dans l'environnement de production. Des tests de pénétration sont réalisés après tout changement important.

Un CCC périodique, qui inclut des représentants de nombreuses équipes d'ADP, est réuni par GETS. Les réunions du CCC se tiennent régulièrement et permettent de discuter des impacts, de convenir des fenêtres de déploiement et d'approuver la promotion des logiciels dans l'environnement de production, ainsi que de communiquer tout changement de l'infrastructure de production.

L'équipe Opérations informatiques d'ADP fournit l'approbation définitive avant la promotion des logiciels vers l'environnement de production.

### Sécurité de l'environnement de développement

Les environnements de développement et de production sont séparés et indépendants l'un de l'autre. Des contrôles d'accès appropriés sont employés pour garantir une séparation correcte des responsabilités. Les logiciels sont accessibles à chaque étape du processus de développement et uniquement par les équipes impliquées dans l'étape en question.

**Données de test**

La politique de gestion des applications d'ADP interdit l'utilisation de données réelles ou non nettoyées dans l'environnement de développement, et les tests sont interdits sauf en cas de demande et d'autorisation expresses du client.

## Section 11 - Relations avec les fournisseurs

### Identification des risques liés aux parties externes

Les évaluations des risques des tiers qui ont besoin d'accéder aux données d'ADP et/ou de clients sont effectuées régulièrement pour déterminer leur conformité aux exigences de sécurité d'ADP pour les tiers, et pour identifier toute lacune dans les contrôles appliqués. Si une lacune de sécurité est identifiée, de nouveaux contrôles sont convenus avec ces parties externes.

### Accords de sécurité des données avec les parties externes

ADP conclut des accords avec tous les tiers qui incluent des engagements en matière de sécurité appropriés pour répondre aux exigences de sécurité d'ADP.

## Section 12 - Gestion des incidents affectant la sécurité de l'information

### Gestion et des incidents affectant la sécurité de l'information et améliorations

ADP a documenté une méthodologie pour répondre aux incidents de sécurité de manière rapide, cohérente et efficace.

En cas d'incident, une équipe prédéfinie d'employés d'ADP met en œuvre un plan de réponse aux indidents officiel qui couvre des domaines tels que :

- L'escalade fondée sur la classification de l'incident ou sa sévérité
- Les coordonnées pour la déclaration/l'escalade des incidents
- Des directives pour les réponses initiales et le suivi avec les clients concernés
- La conformité aux lois relatives à la déclaration des infractions à la sécurité applicables
- Un journal d'enquête
- La restauration des systèmes
- La résolution, la déclaration et l'examen des problèmes
- L'identification des causes profondes et les mesures correctives
- Les leçons apprises

Les politiques d'ADP définissent un incident de sécurité, la gestion d'incident et les responsabilités de tous les employés concernant la déclaration des incidents de sécurité. ADP organise également des formations régulières pour ses employés et entrepreneurs pour les sensibiliser aux exigences de déclaration. Ces formations font l'objet d'une surveillance pour s'assurer qu'elles sont effectivement suivies.

## Section 13 - Aspects de sécurité de l’information liés à la gestion de la résilience des activités

### Programme de résilience des activités d'ADP

ADP s'est engagé à assurer le bon fonctionnement de ses services et opérations, pour fournir à ses clients le meilleur service possible. Notre priorité est d'identifier - et d'atténuer - les risques technologiques, environnementaux, liés aux processus et sanitaires qui pourraient être un obstacle à la prestation de nos services commerciaux. ADP a créé un cadre intégré qui présente nos processus d'atténuation, de préparation, de réponse et de récupération et comprend :

- Évaluation des risques
- Analyse des risques
- Analyse de l'impact sur l'activité
- Élaboration de plans
- Planification de la continuité des activités
- Planification de reprise après sinistre
- Planification de la santé et sécurité
- Réponse pratique
- Gestion de crise
- Réponse d'urgence
- Tests et validation
- Revue
- Révision
- Exercise

## Section 14 - Conformité

### Conformité avec les politiques de sécurité et les normes

ADP emploie un processus visant à réaliser des examens de la conformité internes régulièrement. De plus, ADP réalise une vérification de type II SOC1[2] régulièrement. Ces vérifications sont effectuées par un cabinet de vérification tiers bien connu, et des rapports de vérification sont disponibles chaque année pour les clients sur demande, le cas échéant.

### Conformité technique

Pour garantir la conformité technique avec les meilleures pratiques, ADP réalise régulièrement des examens planifiés de la vulnérabilité du réseau. Les résultats de cet examen sont ensuite classés par ordre de priorité et des plans de mesures correctives sont développés avec les équipes d'hébergement et leurs responsables.

Des examens de vulnérabilité sont effectués régulièrement sur les environnements internes et externes. De plus, des examens du code source et des tests de pénétration sont effectués pour chaque produit. À l'aide d'outils d'examen d'application spécialisés, les vulnérabilités au niveau des applications sont identifiées le cas échéant, communiquées aux équipes de direction du développement de produit, et incorporées dans les processus de contrôle de qualité pour que des mesures correctives soient prises. Les résultats sont analysés, et des plans de mesures correctives sont élaborés et priorisés.

### Conservation des données

La politique de conservation des données d'ADP relative aux données des clients est conçue pour être conforme aux lois applicables. À la fin du contrat d'un client, ADP remplit ses obligations contractuelles associées aux données du client. ADP retourne ou permet au client de récupérer (par téléchargement des données) toutes les informations du client nécessaires à la continuité des activités commerciales du client (si elles n'ont pas été fournies précédemment). Ensuite, ADP détruit de manière sécurisée les informations du client restantes, sauf dans la mesure exigée par la loi en vigueur, autorisée par le client ou nécessaire aux fins d'une résolution de litige.

[2] Dans le cas de certains services américains offerts par ADP, des rapports exécutifs de type II SOC2 sont également disponibles.