Principes de Sécurité et de Protection des Données pour l'entité IBM Technology Support Services

Table des matières

1. Révision de sécurité et de protection des données

Les présents Principes de Sécurité et de Protection des Données pour l'entité IBM Technology Support Services (TSS) sont limités à la description du traitement et de la protection des Données Client par IBM dans ses offres de services de maintenant et support technique (services TSS). Ils décrivent un ensemble général de principes, processus, contrôles et outils qu'IBM utilise pour le traitement de données en interne en rapport avec les données détenues et fournies par le Client identifié dans les documents de transaction, ou collectées par IBM lors de la fourniture de support technique (ci-après, « Données Client »).

1.1 Conformité juridique

IBM respectera toutes les lois et réglementations applicables à ses services TSS, notamment celles applicables à la notification de violation de sécurité. IBM ne détermine pas si les données envoyées à IBM par le Client pour permettre la détermination du problème comprennent des informations soumises à une loi ou une réglementation spécifique. Tous les Incidents de Sécurité sont soumis au Processus de Traitement des Incidents de Sécurité documenté ci-dessous.

1.2 Mises à jour des Principes de Sécurité et de Protection des Données (DSPP) pour les services TSS

Lorsqu'IBM complète ou modifie la portée de ces services TSS par le biais du processus de gestion de modification documentée, IBM peut fournir de nouvelles conditions ou procéder à des mises à jour des DSPP conformément à ces modifications. Lorsqu'un client renouvelle ou achète un nouveau service TSS, les DSPP alors en vigueur s'appliqueront à l'abonnement du Client pour ces services TSS.

1.3 Données Client

Données Client définies

Les Données Client sont une ressource provenant du Client et fournies à IBM à des fins d'accès, de stockage ou de gestion dans le cadre d'un contrat de service TSS. IBM peut entrer en possession des Données Client de plusieurs façons, par exemple : (1) Les clients peuvent utiliser les offres de support produit IBM, (2) Les clients peuvent envoyer des données structurées ou non structurées pour la détermination des problèmes de maintenance et support technique (par exemple, les données de débogage telles que celles contenues dans les vidages mémoire), et (3) Les clients peuvent retourner des machines ou des pièces de machine pour mise à niveau, échange ou réparation, et cet équipement peut contenir des Données Client.

Utilisation des Données Client

Les Données Client ne seront utilisées que pour fournir au Client les services TSS, notamment les activités compatibles avec la fourniture de ces services TSS. IBM n'utilisera pas les Données Client ou ne tirera pas d'informations des Données Client à d'autres fins commerciales sans l'autorisation du Client.

Divulgation des Données Client

Pour les services TSS, IBM utilise parfois ses filiales et ses partenaires commerciaux comme sous-traitants ultérieurs dans les services après-vente et partagera les Données Client avec ces sous-traitants le cas échéant. Dans le cas contraire, IBM ne divulguera pas les Données Client en dehors d'IBM, de ses filiales ou de ses partenaires commerciaux, sauf si le Client le demande ou si la loi l'exige.

Traitement des Données Client

Le règlement général de l'Union européenne sur la protection des données (« RGPD ») exige des accords entre un responsable du traitement et un sous-traitant afin que le traitement soit effectué conformément aux Mesures Techniques et Organisationnelles (« TOM ») du sous-traitant et pour assurer la protection des droits des personnes concernées conformément au RGPD. IBM s'engage à respecter les dispositions du RGPD pour tous les Clients à compter du 25 mai 2018.

1.4 Dispositions du règlement général de l'Union européenne sur la protection des données

a. Les dispositions relatives aux sous-traitants du RGPD s'appliquent au traitement des Données Client dans le cadre du RGPD par IBM, pour le compte du Client.

b. Aux fins des dispositions relatives aux sous-traitants du RGPD, le Client et IBM conviennent que le Client est le responsable du traitement des Données Client et qu'IBM est le sous-traitant de ces données ; lorsque le Client agit en tant que sous-traitant des Données Client, IBM est un sous-traitant ultérieur.

c. Les dispositions relatives aux sous-traitants du RGPD ne s'appliquent pas lorsqu'IBM est un responsable du traitement des Données Client.

d. Les dispositions relatives au sous-traitant du RGPD ne limitent ni ne réduisent les engagements pris par IBM en matière de protection des données à l'égard du Client dans tout autre accord conclu entre IBM et le Client.

2. Principes de Sécurité du Traitement des Données

IBM accorde une priorité élevée à la sécurité des Données Client. La sécurité des installations, personnes et données sont toutes ancrées dans les contrôles métier qui guident l'organisation. Cette section décrit quelques-uns des principes de sécurité sous-jacents qui contribuent aux politiques et procédures de sécurité d'IBM.

IBM se concentre depuis longtemps sur la sécurité via l'utilisation de configurations matérielles et logicielles et via la conception et la mise en œuvre de processus et de pratiques métier. Les menaces peuvent provenir de l'intérieur ou de l'extérieur d'une organisation, de sorte que les procédures et pratiques de sécurité d'IBM tiennent compte d'un large éventail de risques potentiels pour la sécurité des données, notamment des sources technologiques, humaines et naturelles.

L'Instruction interne d'IBM sur la sécurité des technologies de l'information a été élaborée il y a plusieurs décennies et a subi de nombreuses révisions. Elle fournit une structure de surveillance et de contrôle pour l'analyse des risques, la sécurité physique, la gestion des accès, la planification des mesures d'urgence, les investigations, la protection de l'information, l'éducation et plus encore. Elle documente les lignes directrices et les exigences en matière de sécurité informatique et de protection des données, y compris les Données Client. Certaines des exigences documentées dans cette Instruction d'entreprise (entre autres) sont résumées dans les présents DSPP.

2.1 Cloisonnement

Le cloisonnement est une technique qui permet de contrôler les risques associés au comportement humain et consiste à limiter l'accès aux données, tant physique que logique, aux personnes qui en ont réellement besoin pour accomplir leur travail. IBM limite l'accès physique et logique aux centres de données, par exemple aux personnes ayant besoin d'un accès professionnel pour effectuer leur travail. IBM limite l'accès logique aux applications et aux bases de données au personnel autorisé dont la fonction exige l'accès.

2.2 Moindre Privilège

Le Principe du Moindre Privilège indique que le personnel nécessitant un accès ne doit disposer que de l'accès minimum nécessaire pour accomplir sa fonction professionnelle. Ce Principe s'applique aux accès physique et logique aux données, ainsi qu'aux systèmes et applications qui traitent les données. La possibilité de lire, créer, mettre à jour et supprimer des données sont tous des contrôles d'accès soumis au principe du Moindre Privilège.

2.3 Répartition des tâches

La répartition des tâches est un contrôle interne de base qui permet d'éviter un conflit de tâches en ordonnant qu'aucune personne n'ait des responsabilités ou un accès qui lui permettrait d'utiliser ou de détourner les actifs de l'entreprise à mauvais escient ou sans dissuasion ou détection à temps. TSS met en œuvre les concepts de répartition des tâches conformément aux instructions d'entreprise d'IBM en combinant la conception des processus, les contrôles du système et la structure organisationnelle. (Pour une application de ce contrôle, reportez-vous à la rubrique « Élimination des supports et élimination physique des supports » de la Section 3).

2.4 Défense en profondeur

La Défense en profondeur se réfère à la pratique consistant à créer plusieurs couches de sécurité, par exemple, la Défense en profondeur physique exige l'accès par badge à un bâtiment, suivi de l'accès par badge à un centre de données, puis un contrôle d'accès séparé aux cages de serveur du centre de données.

La Défense en profondeur logique correspond à par exemple, plusieurs couches de protection pare-feu comme décrit plus en détails plus loin dans le présent document.

2.5 Confidentialité par conception

La Confidentialité par conception signifie que les principes de protection des données sont incorporés dans la conception d'une activité de traitement dès le début des Services et sont pris en compte tout au long du cycle de vie de chaque offre.

Comme indiqué dans la définition des Données Client, IBM peut recevoir des données non structurées ou non formatées (c'est-à-dire des vidages mémoire ou des captures d'écran) d'un Client afin d'aider le personnel d'IBM à fournir un support après-vente TSS. Le contenu de ces données non structurées peut être inconnu du Client ou d'IBM au moment de la transmission, et peut donc contenir tout élément de données défini dans notre taxonomie standard de données personnelles. IBM mettra en œuvre des TOM pour limiter le traitement des Données Client aux fins autorisées. Seul le personnel IBM autorisé et les sous-traitants ultérieurs autorisés qui ont besoin d'un accès pour entreprendre des tâches autorisées compatibles avec les objectifs autorisés auront accès aux Données Client.

2.6 Gestion des risques informatiques

L'évaluation des risques et la gestion des risques sont les fondements essentiels de la sécurité des données. Le personnel des contrôles internes d'IBM vérifie périodiquement la conformité des contrôles d'entreprise des applications et des processus.

IBM a également un comité directeur de gestion des risques informatiques, dirigé par le Responsable du Système d'Information d'IBM (« CIO »). Les membres du Comité sont des professionnels et responsables de la sécurité ainsi que des personnes qui créent des normes informatiques internes à des fins d'approbation par la direction. Le comité examine en continu les risques informatiques à travers un large éventail de menaces potentielles. Les conclusions de ce Comité sont utilisées pour améliorer l'attitude d'IBM face aux risques informatiques.

3. Sécurité Physique

3.1 Installations et Contrôle d'Accès

La sécurité physique est un aspect clé de la protection des Données Client. IBM emploie des mécanismes de contrôle d'accès pour limiter l'accès aux actifs du système et aux composants de l'infrastructure. Les clés, les verrous de chiffrement, les systèmes d'accès à commande électronique, les entrées surveillées et, dans certains cas, les contrôles biométriques, sont tous des exemples de contrôles d'accès physique pouvant être employés par IBM. Pour les cas où une zone d'accès contrôlé est située dans des locaux n'appartenant pas à IBM, les exigences en matière de sécurité sont détaillées par le biais d'un contrat et le propriétaire de ces locaux accepte de respecter ces exigences.

Les zones d'accès contrôlé sont classées en fonction d'un ensemble de critères définis par le CIO pour identifier et protéger les installations, les contenus et les personnes. L'accès aux zones d'accès contrôlé est consigné et les registres sont examinés par des outils automatisés ou manuellement conformément aux directives de sécurité informatique. La documentation comprenant la preuve de la vérification de la sécurité doit être conservée conformément à la politique mondiale de gestion des enregistrements d'IBM (WRM).

Chaque zone d'accès contrôlé possède un propriétaire désigné responsable du respect des politiques de sécurité. Les zones d'accès contrôlé doivent être verrouillées même lorsqu'elles sont occupées. Les procédures de sécurité spécifiques à un site et applicables à une zone d'accès contrôlé doivent être documentées et testées. L'accès physique autorisé aux zones d'accès contrôlé n'est accordé qu'au personnel doté d'une attestation professionnelle. En fonction des responsabilités professionnelles de cette personne, l'accès peut être restreint à uniquement une partie des installations.

3.2 Supports et retrait physique des supports

Les supports multimédias utilisés pour la sauvegarde, la conservation des dossiers ou la reprise après incident doivent être protégés physiquement contre toute utilisation non autorisée et tout vol et dommage. Seuls des opérateurs agréés sont utilisés pour transférer les supports électroniques pouvant contenir des données non chiffrées.

Les administrateurs des supports de stockage de serveur qui traitent les Données Client sont responsables de l'inventaire exact des supports et de la notification de toute anomalie conformément au et à l'aide du **processus de gestion des incidents de sécurité** d'IBM (SIHP). En accord avec le principe de sécurité de la répartition des tâches, au moins une personne non impliquée dans l'exploitation des supports doit effectuer l'inventaire (l'administrateur des supports de stockage peut y participer mais n'est pas autorisé à être seul responsable de la réalisation de l'inventaire).

La mémoire des machines ou pièces de machine retournées à IBM pour mise à niveau, échange ou réparation qui contiennent des Données Client doit être effacée en toute sécurité par le Client afin de rendre les données irrécupérables avant l'expédition. Si le Client n'est pas en mesure d'effectuer cette tâche pour quelque raison que ce soit, IBM propose des services payants d'effacement sécurisé ou de conservation des supports.

4. Sécurité logique

La sécurité logique est essentiellement constituée de mesures techniques. Quelques mesures de sécurité logiques courantes s'appliquent à l'infrastructure de réseau, aux serveurs et aux postes de travail. Ces mesures comprennent des contrôles d'accès (plus de détails dans les différentes sections ci-dessous) et des mesures techniques pour traiter la propagation ou l'exécution de code non approuvé (p. ex. virus et autres logiciels malveillants). Les mises à jour sont effectuées automatiquement dans la mesure du possible (par exemple, mises à jour d'antivirus de poste de travail) ou périodiquement selon un planning hiérarchisé pré-établi. Voici des exemples de sécurité logique :

- Analyses périodiques de vulnérabilité et test d'intrusion.
- La gestion de patch doit être effectuée dans les meilleurs délais, conformément à une structure de classification de systèmes et du niveau de gravité du patch, voire parfois en fonction du type ou de la version du système d'exploitation.
- Contrôles techniques évitant les attaques par saturation (essentiellement applicables à l'infrastructure réseau et aux serveurs).
- Création et capture, si l'appareil est compatible, des registres de consignation d'activité (infrastructure réseau et serveurs) accessibles à des fins d'audit et aux outils de surveillance d'activité suspecte. La durée de conservation desdits registres de consignation est déterminée par IBM WRM, qui catégorise et détaille les exigences relatives à la conservation. La liste des activités suspectes à surveiller est gérée par le CIO.
- Obligation de conformité aux mesures de sécurité spécifiques pour l'accès distant aux systèmes internes d'IBM depuis l'extérieur du pare-feu logique, y compris un client VPN obligatoire. Tous ces accès sont chiffrés. (Applicable aux postes de travail et aux appareils mobiles).
- Obligation de cataloguer les appareils dans une base de données utilisée pour les activités de contrôle et d'audit.
- Obligation d'utiliser des adresses IP statiques (DHCP/DDNS ne sont généralement pas autorisés, sauf dans certains cas approuvés et documentés pour les serveurs, et pour les postes de travail en général). Toutes les adresses IP statiques sont enregistrées dans une base de données sécurisée.
- IBM exige qu'une politique d'utilisation acceptable soit facilement accessible aux utilisateurs et représentée chaque fois que les conditions changent, demandant confirmation que l'utilisateur a lu et compris les termes des données qui peuvent y être stockées ou traitées.
- Obligation d'utiliser les directives spécifiques du CIO pour générer des images de système d'exploitation (postes de travail ou serveurs), et
- Obligation de se soumettre à des contrôles de sécurité dans le cadre d'un processus d'audit indépendant plus large.

Lorsque la loi l'autorise, un Test Technique de Sécurité (TTS) est effectué par des équipes de personnes hautement spécialisées qui sont autorisées à utiliser leurs compétences, outils et techniques pour détecter les risques potentiels qui ne seraient normalement pas détectés pendant les tests de routine. C'est ce qu'on appelle parfois le test du chapeau blanc ou le piratage éthique. IBM possède des ressources établies aidant les individus à effectuer les tests TTS, y compris la documentation de présentation des processus.

4.1 Spécifications Techniques pour les Serveurs, Middleware et Applications

IBM gère des spécifications techniques détaillées pour la sécurité qui sont spécifiques à chaque système d'exploitation, chaque produit middleware et aux applications déployées. Tous les serveurs de production, les logiciels intermédiaires et les codes d'application utilisés pour fournir un support technique après-vente respecteront ou dépasseront les spécifications définies par le CIO.

4.2 Accès basé sur les rôles

Les services de sécurité interne d'IBM ont mis en place une politique de contrôle d'accès qui décrit les exigences de sécurité en fonction du type de données contenues dans le système, du besoin de savoir

de l'utilisateur, des obligations légales et/ou contractuelles. L'approbation, la vérification et la suppression des demandes d'accès sont formellement définis en tenant compte de ces considérations. IBM maintient une piste d'audit de tous les événements importants concernant les droits d'accès et la gestion des identités.

4.3 Mot de passe et politique d'authentification

Les systèmes de production d'IBM nécessitent un accès authentifié. Il s'agit d'appareils réseau, de serveurs, de postes de travail et de certains types d'application. Certains systèmes nécessitent un ID utilisateur et un mot de passe ou un certificat numérique, d'autres nécessitent une authentification à plusieurs facteurs (par exemple, un mot de passe plus une identification biométrique, ou un mot de passe plus un porte-clés de sécurité). L'authentification à plusieurs facteurs est requise pour tout système disponible sur un réseau public ou pour tout utilisateur privilégié disposant d'une autorité système.

Des règles d'administration de mot de passe sont applicables. Ils doivent comporter un certain nombre de caractères et certaines combinaisons de lettres, casses, chiffres et autres caractères spéciaux. En outre, des règles de tentative de saisie de mot de passe incorrecte sont en vigueur, par exemple en interdisant l'accès au bout d'un certain nombre de tentatives infructueuses. Les outils automatisés (le cas échéant) rappellent aux utilisateurs de changer leurs mots de passe et d'appliquer les règles d'administration de mot de passe.

Les mots de passe sans expiration ne sont généralement pas autorisés, à de très rares exceptions près (par exemple, les mots de passe de disque dur d'ordinateur portable sont des exceptions, mais ces mots de passe n'interviennent que si un disque dur est retiré puis reconnecté à un contrôleur « étranger »). Les certificats numériques utilisés pour l'identification doivent émaner d'une autorité de certification agréée par le CIO d'IBM.

4.4 Sécurité réseau

La sécurité réseau implique des mesures de sécurité physiques et logiques. Sur le plan de la sécurité logique, IBM partitionne son infrastructure informatique en zones de sécurité comprenant des unités de contrôle de flux, telles que pare-feux et routeurs, régissant les flux admissibles entre les zones de sécurité. Ainsi, IBM peut déployer une architecture conforme au principe de sécurité Défense en Profondeur décrit ci-avant.

Il existe des restrictions de sécurité physique quant au placement physique des appareils d'infrastructure réseau dans les zones d'accès contrôlé. Tout système connecté à un réseau non sécurisé, tel qu'Internet, est hautement restreint. Les connexions établies à partir de ces systèmes hautement restreints à tout autre système de production chez IBM sont rigoureusement contrôlées. Des pare-feux sont spécifiés à plusieurs niveaux dans l'architecture de réseau. Des ensembles de règles de pare-feux obligatoires sont établis.

Des mesures techniques limitant la propagation ou l'exécution d'un code non approuvé (par exemple, virus ou autres programmes malveillants) sont requises pour tout appareil d'infrastructure si possible. Les routeurs, les commutateurs et les points d'accès filaires et sans fil sont soumis à un contrôle d'accès, ainsi que les serveurs et les postes de travail. Aucun point d'accès sans fil non sécurisé n'est autorisé (à quelques exceptions près pour l'accès invité non sécurisé à Internet). L'accès par le personnel autorisé est limité aux personnes dont le rôle professionnel nécessite un accès. Les utilisateurs ordinaires n'ont pas accès aux appareils de l'infrastructure réseau.

4.5 Sécurité Serveur

Des contrôles logiques et physiques s'appliquent aux systèmes de serveur de production. De nombreux contrôles techniques sont requis pour les serveurs, en fonction des catégories d'utilisation de serveur. Le CIO IBM gère un ensemble de règles de sécurité de niveau hyperviseur ainsi que des spécifications techniques complètes et détaillées pour les paramètres de sécurité par système d'exploitation de serveur.

L'accès serveur est en fonction des besoins. Comme partout, les règles d'autorisation serveur suivent le principe de moindre droit d'accès, où le niveau minimal de droit d'accès correspondant au besoin professionnel est accordé. En particulier, les privilèges « superutilisateur » ou équivalents sur les serveurs de production ne sont pas accordés aux utilisateurs ordinaires.

Les administrateurs de serveur ou toute personne disposant de privilèges d'accès administrateur sont soumis à davantage d'exigences de sécurité que les utilisateurs ordinaires.

4.6 Sécurité de base de données

Le CIO IBM gère des spécifications techniques complètes et détaillées pour les paramètres de sécurité du logiciel intermédiaire de base de données. A l'instar des serveurs en général, les bases de données sont soumises à des exigences de contrôle physiques et logiques. Les bases de données doivent avoir plusieurs niveaux de contrôle d'accès, qui peuvent également varier selon la sensibilité des données qu'elles contiennent. Les administrateurs de base de données, comme tout autre utilisateur disposant de privilèges élevés, sont soumis à davantage d'exigences de sécurité que les utilisateurs ordinaires.

4.7 Sécurité des postes de travail et des appareils portables

Les employés d'IBM doivent respecter des règles spécifiques concernant les postes de travail éventuellement utilisés pour accéder aux Données Client. Ces postes de travail doivent présenter les caractéristiques suivantes :

- être équipés d'un mécanisme de protection antivirus à jour prescrit par le CIO (un logiciel antivirus spécifique est obligatoire). Les analyses antivirus sont obligatoires et automatiquement programmées ;
- être équipés d'un système de protection par mot de passe activé lors de la connexion ;
- avoir un délai de verrouillage de clavier/écran paramétré sur 30 minutes ou moins (15 minutes dans certains cas) ;
- utiliser l'option de chiffrement pour toutes les bases de données Lotus Notes pouvant contenir des informations sensibles ;
- si l'appareil prend en charge un mot de passe d'accès au disque dur, il doit être activé, sauf si le chiffrement intégral de disque dur est utilisé ;
- être automatiquement mis à jour à l'aide des patch de sécurité ;
- ne contenir aucun logiciel ou donnée non approuvé ou inapproprié ;
- n'utiliser que des logiciels Open Source pré-approuvés. Le processus d'approbation vise à garantir que seuls des logiciels testés et sécurisés sont utilisés et qu'IBM respecte les conditions d'utilisation applicables ;
- être équipés de logiciels de surveillance spéciaux pouvant vérifier la conformité aux exigences de sécurité et aider IBM à gérer les appareils des utilisateurs finaux (par exemple, Tivoli End Point Manager) ;
- être équipés d'un logiciel VPN (Virtual Private Network) approuvé par le CIO pour l'accès à distance à l'intranet d'IBM. Cet accès est chiffré selon la puissance de chiffrement définie par le CIO ;
- être équipés d'un pare-feu client approuvé par IBM et opérationnel ;
- ne pas utiliser d'applications de partage de fichiers poste à poste au travers d'Internet, sauf accord du CIO ;
- n'autoriser aucune forme d'accès non authentifié ou non approuvé ;
- avoir une adresse MAC enregistrée, et
- obtenir des versions agréées des logiciels requis par IBM auprès d'un système de distribution de logiciel interne (appelé ISSI, IBM Standard Software Installer) ;

IBM se réserve le droit de confisquer tout actif personnel (ordinateurs ou téléphones portables, par exemple) qui est utilisé en intégralité ou en partie aux fins professionnelles d'IBM. Ces confiscations peuvent être effectuées, par exemple, dans le cadre d'une investigation.

4.8 Sécurité d'application

Les administrateurs d'application sont soumis à davantage d'exigences de sécurité que les utilisateurs ordinaires, en raison de leur niveau d'autorisation amélioré. Les applications nécessitent une authentification et une autorisation, similaires à mais malgré tout distinctes de la connexion de système d'exploitation.

4.9 Prévention contre les intrusions, détection et analyse de vulnérabilité

La prévention contre les intrusions est obligatoire. Des contrôles de logiciel anti-programmes malveillants sont nécessaires à plusieurs niveaux (plusieurs niveaux dans l'architecture de réseau, le serveur et le poste de travail). Des pare-feux sont spécifiés à plusieurs niveaux dans l'infrastructure réseau ainsi que pour les serveurs et les postes de travail.

La détection d'activité suspecte est obligatoire. La plupart des activités et accès sont surveillés et consignés dans le cadre de la détection d'activité suspecte. Les utilisateurs ayant des privilèges élevés sont davantage surveillés. La liste des événements du registre de sécurité est gérée par le CIO.

L'analyse de vulnérabilité est effectuée selon un planning lié au type du système à analyser. Les systèmes connectés à Internet qui sont considérés être vulnérables sont retirés du service sauf s'ils peuvent être corrigés avec des délais déterminés.

Des outils d'analyse agréés sont disponibles pour téléchargement par les administrateurs système et les professionnels de la sécurité à partir du site Web SRAM (Security, Asset, and Risk Management) interne. Les profils d'analyse de vulnérabilité requis sont également stockés sur ce site.

5. Ingénierie sécurisée

L'**infrastructure d'ingénierie sécurisée d'IBM** reflète les efforts économiquement raisonnables et oriente les équipes de développement pour porter une attention toute particulière à la sécurité pendant le cycle de développement.

Les pratiques d'ingénierie sécurisée sont les suivantes : planification de projet, formation en matière de sensibilisation à la sécurité, évaluation des risques et modélisation des menaces, exigences de sécurité, codage sécurisé, analyse de code source et test de sécurité dynamique, documentation relative à la sécurité et un processus d'intervention en cas d'incident lié à la sécurité du produit. Ces pratiques aident à améliorer la sécurité du produit, à protéger la propriété intellectuelle IBM et à prendre en charge les conditions de garantie des produits IBM. Pour en savoir plus sur la sécurité des produits IBM, voir : http://www.ibm.com/security/secure-engineering/ http://www.ibm.com/security/secure-engineering/process.html.

6. Processus de Traitement des Incidents de Sécurité

IBM gère un système unique de notification et d'atténuation des incidents de sécurité où les incidents de sécurité et de données informatiques pouvant compromettre (1) les informations personnelles, les informations client et les informations techniques ou scientifiques IBM confidentielles ou (2) un appareil de productivité ou (3) une activité informatique suspecte ou (4) une intrusion suspecte dans le système communiquée à un point de contact téléphonique/Web unique.

Ce rapport déclenche une intervention de la part d'une équipe d'employés spécialement formés et équipés disponibles 24h/24 et 7j/7 toute l'année qui, en collaboration avec les équipes de la division logicielle et d'autres spécialistes selon les besoins, géreront l'incident jusqu'à sa résolution.

Des intervenants spécialisés ont été désignés pour chaque division de sorte que, si un incident se produit, un processus de traitement des incidents de sécurité (SIHP) est également appelé pour garantir qu'une intervention rapide pour les incidents de sécurité, conformément aux exigences de notification de l'entreprise, a lieu.

IBM prend en charge les exigences de production de rapports du RGPD et signalera toute violation des données dans un délai de 72 heures en tant que contrôleur ou sous-traitant. Ces exigences de production de rapports comprendront :

- une description de la nature de la violation des Données Client, y compris, dans la mesure du possible, les catégories et le nombre approximatif de personnes concernés ainsi que les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact où l'on peut obtenir davantage d'informations ;
- les conséquences probables de la violation des Données Client et,
- les mesures prises ou envisagées par le responsable du traitement pour remédier à la violation des Données Client, y compris, le cas échéant, des mesures visant à en atténuer les effets négatifs éventuels.

7. Pratiques en matière d'emploi liées à la sécurité des données

La protection des Données Client dépend des moyens techniques et autres décrits ci-dessus et du personnel qui gère les données. Les pratiques en matière d'emploi sont conçues pour garantir que tous les employés et sous-traitants respectent un ensemble de directives et peuvent être, dans les limites des lois applicables, surveillés dans le cadre de leurs activités professionnelles.

7.1 Politiques de recrutement et de rupture de contrat

Lorsque la loi le permet, la vérification préalable à l'emploi comprend le contrôle des antécédents, la vérification du niveau d'étude présenté, la vérification de la carte d'identité avec photo établie par le gouvernement et la vérification des autres demandes d'emploi. Les politiques de rupture de contrat exigent le retrait de l'accès réseau (objectif : moins de 24 heures). Les employés objet d'une rupture de contrat doivent restituer les biens d'IBM, y compris les postes de travail, les ordinateurs portables, les supports appartenant à IBM et tout équipement de communication. L'obligation permanente de confidentialité de données est rappelée aux employés objet d'une rupture de contrat.

7.2 Formation et Culture

Les nouveaux employés reçoivent une formation qui comprend l'utilisation adéquate des actifs informatiques et la protection des données sensibles. Une formation annuelle définie par le CIO aux menaces numériques et à la sécurité est obligatoire pour tous les employés.

7.3 Conformité aux Politiques

IBM conserve un code de conduite destiné aux employés, y compris les Principes de Conduite dans les Affaires. Ces principes sont gérés par le Directeur Juridique d'IBM. Les Principes de Conduite dans les Affaires exigent que les employés d'IBM exercent leurs activités à l'aide de normes éthiques rigoureuses et conformément aux politiques de sécurité et de confidentialité de données. Les employés sont invités à communiquer tout comportement illégal ou immoral réel ou apparent.

Les employés doivent lire et accepter les Principes de Conduite dans les Affaires lors du recrutement et chaque année par la suite. La conformité aux Principes de Conduite dans les Affaires est une condition d'emploi. IBM met les Principes de Conduite dans les Affaires à la disposition du public à l'adresse suivante : http://www.ibm.com/investor/governance/business-conduct-guidelines.wss.

7.4 Programme En toute confidentialité

Afin de protéger les Données Client, les employés doivent pouvoir porter les problèmes à l'attention de la direction à tout moment. IBM a mis en place des programmes permettant cette liberté afin d'identifier et communiquer tout problème potentiel.

8. Contrôles d'entreprise, Instructions d'Entreprise, Normes CIO

IBM utilise le cadre du Committee of Sponsoring Organizations de la Commission Treadway (« COSO ») et ses cinq composants interdépendants : l'environnement de contrôle, l'évaluation des risques, les activités de contrôle, l'information et la communication, et le suivi.

Des politiques et des pratiques uniformes sont établies sous la forme de directives d'entreprise qui sont la principale méthode permettant à IBM de documenter et communiquer efficacement ses politiques, délégations et instructions à la direction et aux employés d'IBM. Les politiques de sécurité informatique tirent leur autorité des instructions d'entreprise spécifiques et d'autres sources de contrôle métier faisant autorité et, à ce titre, font partie intégrante des activités d'IBM.

9. Audit

La sécurité des Données Client est fonction des contrôles mis en œuvre et vérifiés. L'une des façons de réaliser la vérification est de procéder à des audits indépendants de l'unité qui effectue le travail. IBM audite régulièrement la conformité aux contrôles métier, y compris aux contrôles informatiques (l'audit vérifie que les normes et politiques de sécurité sont en conformité). Les Contrôles Métier et la fonction d'Audit Internet relèvent du directeur financier d'IBM, qui rend compte au Comité d'Audit du Conseil d'Administration.

10. Continuité des Opérations

Toutes les fonctions essentielles à l'exercice des activités d'IBM sont associées à des plans de reprise après incident. Ces plans formels sont documentés et revalidés tous les ans (au minimum). Les services de notification et de résolution des problèmes techniques, qui dépendent des Données Client, sont critiques et sont associés à des plans de reprise après incident.

11. Gestion de crises

IBM gère un processus de gestion de crises dans le cadre d'un Programme de Planification d'Urgence, conçu pour permettre à IBM de traiter les crises à mesure qu'elles se présentent. Ce processus nécessite des sites/locaux d'IBM et le personnel compétent pour créer un Plan d'Urgence. Le processus de gestion de crises est activé immédiatement lorsqu'une situation de crise réelle ou potentielle se présente.

12. Service et Support

Les Clients peuvent être invités à fournir (ou peuvent choisir d'envoyer volontairement) des données aidant IBM à déboguer un problème. Les Clients seront invités à utiliser l'outil en ligne sécurisé (connu sous le nom Enhanced Customer Data Repository, ECuRep) pour envoyer les données de débogage à IBM. L'outil ECuRep et ses conditions d'utilisation sont décrites à l'adresse suivante : http://www.ibm.com/de/support/ecurep

13. Acquisitions

IBM se réserve le droit d'acquérir d'autres sociétés dont les politiques et procédures existantes en matière de sécurité de Données Client diffèrent de celles d'IBM. Les sociétés acquises doivent se conformer aux mêmes politiques de sécurité qu'IBM dans un délai d'intégration ou de transition défini suivant l'acquisition. Les mêmes contrôles physiques, logiques et métier appliqués dans toute l'entreprise d'IBM s'appliqueront à la société acquise avant la fin du délai d'intégration. La durée requise pour la période d'intégration est fonction de la complexité de l'infrastructure existante de la société acquise.