NORMES EN MATIÈRE DE SECURITÉ INFORMATIQUE POUR LES FOURNISSEURS

VERSION DETAILLÉE

OBJECTIF

L'objectif des normes en matière de sécurité informatique est de protéger efficacement l'information de Computacenter et de ses clients, en offrant une stratégie flexible et cohérente à la fois en ce qui concerne la gestion de la sécurité de l'information. Elles aident également les fournisseurs de Computacenter à mieux comprendre et à coopérer dans le cadre des contrôles de sécurité appropriés. Les normes en matière de sécurité informatique pour les fournisseurs définissent le niveau minimal des exigences du contrôle de sécurité à atteindre pour les fournisseurs. Cela comprend tous les éléments impliqués dans la prestation des services ou produits à Computacenter ou à ses clients.

Le fournisseur fera l'objet d'une nouvelle évaluation au regard des normes en matière de sécurité informatique de Computacenter au premier des cas suivants : a) lors de la modification substantielle de tout aspect relatif aux opérations du fournisseur, ou b) au moins une fois tous les deux ans.

Tous les nouveaux fournisseurs devront respecter les conditions pertinentes de cette norme (selon les produits et services fournis à Computacenter et à ses clients). En cas de conflit direct entre les exigences de cette norme et les conditions d'un accord écrit (entre le fournisseur et Computacenter), les conditions du contrat écrit prévaudront sur les exigences.

CHAMP D'APPLICATION

Le champ d'application de cette norme inclut tout fournisseur qui traite les actifs et l'information de Computacenter ou de ses clients, ou qui peut y accéder. Ce qui comprend, entre autres :

- Les fournisseurs qui traitent, retiennent, transmettent des données pour Computacenter ou ses clients, ou qui y accèdent
- L'accès à l'environnement Computacenter à partir de sites distants où nos équipements informatiques ne sont pas sous le contrôle de Computacenter
- Le personnel du fournisseur ayant besoin d'accéder à des données de Computacenter ou de ses clients, ou à tout élément des systèmes informatiques
    - Cette norme s'applique donc à tout le personnel (y compris les sous-traitants et les intérimaires) employé de façon directe ou indirecte par le fournisseur.

1. GOUVERNANCE DE LA SÉCURITÉ DE L'INFORMATION

Le fournisseur veillera à ce que :

- une ou plusieurs personne(s) soi(en)t désignée(s) responsable(s) du programme de sécurité de l'information de l'entreprise ainsi que de la conformité continue aux exigences de son entreprise par rapport aux normes en matière de sécurité informatique de Computacenter ;
- les politiques de sécurité de l'information de son entreprise soient créées, approuvées, révisées chaque année et communiquées au personnel ;
- la gouvernance de la sécurité de l'information soit activement déployée pour surveiller et évaluer l'efficacité des mesures de sécurité, et en informer la direction du fournisseur.

2. CONFORMITÉ ET EFFICACITÉ

Computacenter demande au fournisseur de se conformer aux exigences et d'exprimer son engagement envers la sécurité de l'information et l'efficacité des mesures de sécurité. Des rapports seront élaborés avec toutes ces données et transmis à Computacenter sur demande. Ces garanties seront basées sur des auto-évaluations concernant les risques sur les données et les contrôles de sécurité menées par le fournisseur.

- Tout le personnel du fournisseur impliqué dans la prestation de services à Computacenter, ou à ses clients, ou ayant accès à leurs données ou aux sites de Computacenter doit, au minimum :
    - mettre en place les meilleures pratiques en matière de sécurité de l'information sur l'ensemble des composants et des matériels fournis, y compris les logiciels et ses contenus, afin de protéger la confidentialité, la disponibilité et l'intégrité des données de Computacenter et de ses clients ;
    - lire, comprendre et s'assurer d'être en conformité avec la politique de bon usage de l'informatique de Computacenter ;

- classifier et gérer tout actif porteur d'informations protégées conformément aux exigences de classification et traitement de l'information tel qu'indiqué dans les politiques de Computacenter.

Si un fournisseur doit respecter les politiques de sécurité spécifiques à un client, Computacenter doit remettre au fournisseur les politiques en question.

3. EXTERNALISATION DES SERVICES À UNE TIERCE OU À UNE QUATRIÈME PARTIE

Le fournisseur n'est pas autorisé à sous-traiter les services (en tout ou en partie) inclus dans le contrat avec une tierce ou avec une quatrième partie, sans le consentement écrit de Computacenter. Dans les cas où Computacenter a approuvé la sous-traitance de certaines activités du fournisseur, le sous-traitant n'est pas autorisé à externaliser les services d'avantage sans le consentement écrit de Computacenter.

Le fournisseur se chargera (dans le cadre de sa stratégie de gestion de la sécurité de l'information) que la base de la chaîne d'approvisionnement soit sous contrôle, et que les exigences contractuelles relatives aux normes de sécurité soient imposées tout au long de la chaîne d'approvisionnement du fournisseur. Les preuves des évaluations relatives aux normes de sécurité effectuées pour des services de tiers (où les données de Computacenter sont stockées ou traitées), dont, entre autres, les rapports des évaluations indépendantes sur la sécurité disponibles et élaborés par une tierce partie, doivent être transmises à Computacenter sur demande, comme la certification ISO27001 ou les rapports SOC-2.

4. ATTÉNUATION DES RISQUES POUR LA SÉCURITÉ DE L'INFORMATION

Le fournisseur doit assurer une stratégie appropriée de la gestion des risques en matière de sécurité de l'information (pour identifier les risques provoqués par les services informatiques) à l'équipe de sécurité de l'information de Computacenter. Le fournisseur doit documenter et évaluer tous les risques identifiés, et proposer des mesures de protection.

Ainsi, le fournisseur doit collaborer avec Computacenter pour maintenir un plan de sécurité comprenant les mesures de limitation des risques ainsi que l'efficacité de ces mesures en ce qui concerne les risques identifiés pour la sécurité de l'information de Computacenter. Le fournisseur produira le registre des risques avec Computacenter, dans lesquels se trouveront les risques identifiés concernant la sécurité de Computacenter et de ses clients, dans le cadre de la prestation de produits et services convenue. Il fournira ce registre sur demande et dans un délai raisonnable.

5. CONTRÔLE D'IDENTITÉ, CONTRÔLE DE SÉCURITÉ, VÉRIFICATION ET FILTRAGE

Le fournisseur veillera à ce que tout le personnel du fournisseur qui :

- accède physiquement aux sites Computacenter,
- accéde à distance aux données de Computacenter ou à celles de ses clients,

respecte la politique de bon usage de l'informatique de Computacenter et les politiques supplémentaires au niveau local et/ou spécifiques au service, selon les besoins. Lors du recrutement, le fournisseur est tenu d'effectuer une inspection/filtrage préalable du personnel.

Computacenter peut effectuer des contrôles supplémentaires du parcours du personnel du fournisseur, en fonction des exigences spécifiques au poste ou des besoins individuels du client.

6. FORMATION DU PERSONNEL

Pendant la prestation de services à Computacenter ou à ses clients, le fournisseur veillera à ce que ;

- les formations de sensibilisation à la sécurité soient une partie intégrante du programme d'accueil et de formation pour tous les employés existants ou nouveaux ;
- tout le personnel soit conscient des menaces et préoccupations associées à la sécurité de l'information, de sa part de responsabilité à cet égard et qu'il soit doté des outils nécessaires pour soutenir les politiques en matière de sécurité de l'entreprise ;
- les formations et séances d'information soient évaluées régulièrement.

Computacenter peut demander à son fournisseur de fournir un rapport sur le statut de la formation donnée à ses collaborateurs délivrant des services à Computacenter et à ses clients.

7. AUDIT CONCERNANT LA SÉCURITÉ

Computacenter aura le droit, à condition de donner un préavis raisonnable, de mener un audit concernant la sécurité de l'information afin d'évaluer la conformité du fournisseur aux exigences de l'accord et des services offerts par Computacenter dans le site du fournisseur ou par un prestataire de services d'audit externe. Les audits seront effectués au moment et dans le champ d'application convenus. La conformité aux exigences du service et contractuelles sera vérifiée dans le cadre d'un audit. Les résultats de l'audit seront vérifiés et suivis par le fournisseur.

En cas d'écart ou non-conformité lors des auto-évaluations sur les risques et la sécurité de l'information, ou pendant les audits sur les services du fournisseur, ce dernier se chargera de mettre en place des mesures correctives appropriées pour limiter des risques en temps opportun, ainsi que de faire rapport des objectifs atteints auprès de Computacenter.

8. APPROVISIONNEMENT, DÉVELOPPEMENT ET MAINTENANCE DES SYSTÈMES INFORMATIQUES ET LOGICIELS

8.1. EDITION DE LOGICIELS

Pour ce qui est de l'approvisionnement de logiciels associés aux services destinés à Computacenter ou à ses clients, le fournisseur veillera à ;

- ce que le logiciel ne contienne aucune vulnérabilité connue, comme par exemple, celle décrite dans la dernière version OWASP[1] (Open Web Application Security Project) Top Ten most critical Web application vulnerabilities ;
- adopter les meilleures pratiques OWASP (par exemple les directives pour les tests OWASP, modèles de maturité OWASP) ;
- mettre en place les processus reconnus par le secteur tels que SDLC (Software Development Life Cycle) afin d'assurer la couverture de garantie et la facilité d'utilisation ;
- garantir que tout logiciel fourni ou utilisé ne contienne aucun programme malveillant (y compris les virus sur les ordinateurs, vers informatiques, portes dérobées, chevaux de Troie et tout autre type de programmes malveillants) qui affaiblisse la sécurité de l'application ;
- assurer que seuls des logiciels qui puissent être examinés indépendamment soient fournis (afin de garantir qu'ils répondent aux attentes) et ne contiennent aucune des faiblesses ou vulnérabilités connues ;
- garantir que tout code (y compris des tierces parties) soit testé avant d'être exécuté dans l'environnement de production, et qu'une copie en local soit produite et non pas seulement référencée comme un assembly distinct ;
- divulguer, à la demande de Computacenter, tous les logiciels de tierces parties utilisés, y compris les bibliothèques, les cadres de référence, les composants et autres produits, qu'ils soient commerciaux, gratuits, des logiciels ouverts ou fermés ;
- donner les précisions nécessaires sur le(s) produit(s) ou service en fin de vie, sans oublier les options de mise à jour permettant à Computacenter d'évaluer tout risque concernant la sécurité et les options viables pour limiter ces risques.

Le fournisseur accepte d'offrir un soutien raisonnable à l'équipe de révision de Computacenter grâce à l'accès au code source. Le fournisseur offrira des conventions d'entiercement de logiciels pour le code source là où le code source du logiciel n'est pas fourni par Computacenter dans le cadre de l'accord.

8.2. ACCÈS À DISTANCE

Si le fournisseur doit accéder à l'environnement informatique de Computacenter à distance, il devra se conformer aux normes suivantes en ce qui concerne la prestation des services ou produits à Computacenter :

- Le fournisseur ne pourra accéder à l'environnement informatique de Computacenter qu'à travers le système d'accès à distance (Remote Access System ou RAS)2, qui ne peut être utilisé qu'à des fins d'exécution des obligations contractuelles visant à offrir les produits et services à Computacenter.
- Accès par le biais d'un modèle d'accès à distance de type "concierge ", par partage d'écran avec un employé de Computacenter permettant uniquement l'accès au système pendant la période requise.

---

[1] Consultez le Web Application Security Project Top Ten Security Risks disponible sur World Wide Web

[2] Système d'accès à distance (RAS) - Solutions technologiques du centre informatique pour obtenir un accès à distance.

- Les fournisseurs doivent mettre en place des mesures de sécurité afin de protéger leurs environnements informatiques contre tout risque de sécurité (entre autres les vulnérabilités, les menaces pour la sécurité ou les virus malveillants) associées à l'utilisation d'une solution d'accès à distance2.
- Le fournisseur doit mener les contrôles de sécurité appropriés (techniques, procéduraux, et organisationnels) pour empêcher une utilisation non autorisée et identifier de manière positive tous les utilisateurs de leur infrastructure informatique dans leurs locaux, conformément à la politique d'identité, d'accès et de gestion des mots de passe de Computacenter.
- L'usage n'est permis que pour un support valide pour incidents, ou pour une demande de changement approuvée formellement enregistrée par Computacenter sur un système de support du fournisseur3.
- Le fournisseur doit traiter l'information en respectant la politique de traitement et de classification de l'information lorsqu'il partage son écran avec les collaborateurs de Computacenter (lors de sessions WebEx, par exemple).
- Le fournisseur est responsable des actions menées telles que l'utilisation des comptes d'utilisateur sur l'environnement informatique de Computacenter.
- Le personnel du fournisseur ou le propriétaire des actifs devra obtenir l'autorisation pour installer le logiciel requis permettant d'accéder au système d'accès à distance2 de Computacenter. Computacenter n'est pas propriétaire du logiciel, ni n'offre de licence ou du support pour le logiciel requis pour accéder au système d'accès à distance2.
- Computacenter se réserve le droit de désactiver ou suspendre l'accès du fournisseur au système d'accès à distance2pour une raison quelconque et sans préavis. Computacenter reconnaît que si le fournisseur ne peut accéder à la solution d'accès à distance2 en raison d'une suspension ou d'une désactivation, tous les niveaux de service pertinents ne s'appliqueront pas pendant la période où il n'est pas en mesure d'utiliser la solution RAS2.
- La solution RAS2 peut servir à transférer les données à partir de ou vers l'infrastructure informatique de Computacenter. Il est interdit au personnel du fournisseur de copier les données de Computacenter ou de ses clients, stockées sur les systèmes informatiques et/ou de transférer ces données sur les dispositifs du fournisseur, ou sur tout autre lieu de stockage hors de l'infrastructure informatique de Computacenter sans l'autorisation écrite explicite de Computacenter.
- L'accès ou l'utilisation du système d'accès à distance de Computacenter2 sera bloqué dès la fin du contrat avec le fournisseur.

8.3. EXIGENCES PAR RAPPORT À L'ÉCHANGE D'INFORMATION

- Les fournisseurs doivent respecter à tout moment la politique en matière de sécurité de l'information de l'entreprise approuvée par l'administration, ou l'ensemble de politiques de sécurité qui définissent les responsabilités et stratégies concernant la sécurité de l'information.
- Accès par le biais d'un modèle d'accès à distance de type "concierge4", par partage d'écran avec un employé de Computacenter permettant uniquement l'accès au système pendant la période requise.
- Les données de Computacenter ou de ses clients sont classifiées en fonction des critères définis dans le cadre de la politique de bon usage de l'informatique de Computacenter (chapitre : traitement et de classification des informations / politique de traitement et de classification des informations). La classification détermine les exigences pour la protection des données lorsqu'elles sont transmises et stockées électroniquement.
- Computacenter et le fournisseur se sont mis d'accord pour définir la méthode pertinente pour l'échange électronique d'information en ce qui concerne la prestation de produits et services à Computacenter ou à ses clients.
- Le fournisseur ne peut copier (sur papier ou électroniquement) toute information et/ou donnée de Computacenter ou de son client sans l'autorisation explicite de Computacenter.
    - L'autorisation de procéder doit être enregistrée dans un registre de transfert d'informations (ou Information Transfer Log).

Veuillez noter que les échanges ad hoc et les communications commerciales générales sont exclues de cette définition.

8.4. UTILISATION DE SERVICES BASÉS SUR LE CLOUD PAR LE FOURNISSEUR POUR LE TRAITEMENT DES DONNÉES

- Le stockage et le traitement des données de Computacenter par le fournisseur grâce à des plateformes de technologie de diffusion basées sur le cloud d'une tierce partie (comme l'Infrastructure as a service ou IaaS, la Platform as a service ou PaaS et le Software as a service ou SaaS) doivent respecter les exigences de sécurité indiquées dans ce document.

---

[3]Le système de support du fournisseur inclut les outils du Service Desk servant à gérer les incidents, les changements et les demandes.

[4] Partage d'écran - à l'aide d'outils tels que Microsoft Teams - Cette méthode est nécessaire lorsqu'une habilitation de sécurité spécifique est requise pour le soutien technique et que le tiers doit être surveillé par un employé de Computacenter ayant l'habilitation appropriée.

- Les fournisseurs qui offrent un service cloud doivent élaborer un processus pour la destruction des données et assurer que toutes les données de Computacenter requises soient supprimées correctement. Cela inclut un processus de désinfection (réduction à zéro ou zeroing out) des conteneurs de stockage et la suppression des données éphémères.
- Les fournisseurs qui offrent des services cloud doivent suivre une méthode pour chiffrer les données sensibles stockées et pendant leur transfert selon les meilleures pratiques industrielles du secteur.
- Les fournisseurs qui offrent des services cloud doivent manipuler les données et actifs de Computacenter ou de ses clients de manière sécurisée, en assurant un isolement logique et une migration sécurisée.
- Les fournisseurs offrant un service cloud doivent inclure des méthodes ou options qui permettent l'authentification multi-facteurs pour les rôles administrateur cloud et selon les exigences de Computacenter ou de ses clients. De plus, Computacenter prévoit que le prestataire de services cloud mette en place les meilleures pratiques telles que l'authentification multi-facteurs pour le contrôle d'accès aux systèmes de gestion de l'infrastructure du prestataire de services.
- Les fournisseurs doivent respecter les politiques d'identité, d'accès et de gestion des mots de passe et les politiques de bon usage de l'informatique de Computacenter.
- Les fournisseurs offrant un service cloud doivent avoir une copie des audits ou des feuilles de route de la conformité aux exigences alignées avec les certifications standard du secteur concernant la sécurité cloud (notamment ISO270017, NIST.SP.800-144, Cloud Computing Compliance Controls Catalogue (C5), CSA STAR, SSAE16, FEDRAMP, FIPS 140-2, et Open Data Alliance)
- Les services basés sur le cloud doivent démontrer comment ils répondent aux exigences BC/DR[5].
- Le fournisseur doit révéler si l'information est traitée hors de l'Espace Economique Européen (EEE)

8.5. LA SÉCURITÉ DE L'INFRASTRUCTURE INFORMATIQUE DU FOURNISSEUR

Les fournisseurs doivent respecter les normes de sécurité de Computacenter par rapport à leur infrastructure impliquée dans la prestation de produits et services à Computacenter.

- Le fournisseur doit appliquer les normes et processus qui garantissent la confidentialité, l'intégrité et la disponibilité de l'information et des services, sans perdre de vue les nouvelles menaces et vulnérabilités (grâce à un processus d'évaluation de risques favorisant la mise en place de limitation des risques en temps voulu).
- Les fournisseurs doivent maintenir un contrôle et une visibilité suffisants de tout ce qui est relatif à la sécurité des informations sensibles ou critiques, ou aux installations de traitement de l'information auxquelles ils accèdent, qu'ils traitent ou gèrent grâce à des processus tels que la gestion des changements, la gestion des vulnérabilités/menaces et la gestion des incidents de sécurité informatique.
- Le fournisseur doit définir le processus de fin de vie (end of life ou EOL) pour tous les composants de l'infrastructure. Il pourrait inclure la date EOL et tous les déclencheurs commerciaux qui pourraient avoir une incidence sur la date EOL.
- Toute donnée à caractère personnel (Personal Identifiable Information ou PII) sensible transmise doit être sécurisée correctement. Le système ne peut transférer des PII à d'autres systèmes. Ces données ne peuvent être utilisées à des fins autres que celles spécifiées, sauf autorisation explicite de Computacenter ou des individus à qui appartiennent ces données.
- Les segments de réseau connectés à Internet doivent être protégés par un pare-feu, configuré de façon à protéger tous les dispositifs associés en abordant toutes les menaces à la sécurité connues.
- Les applications, les ports, les services et les autres points d'accès installés sur un ordinateur ou sur les infrastructures locales, qui ne sont pas nécessaires à la prestation des services à Computacenter, doivent être désactivés ou supprimés.
- La connexion extranet sur le réseau Computacenter doit se faire uniquement à travers des connexions à distance sécurisées approuvées et autorisées par Computacenter.
- Le fournisseur est responsable de la mise en place des protocoles sécurisés dans ses locaux ainsi que de la gestion des protocoles grâce à un processus de contrôle des changements.
- Les systèmes doivent avoir la capacité de détecter une possible attaque. Parmi lesquels se trouvent Network Intrusion Detection (NID), Host Intrusion Detection (HID) / Prevention. Tous les systèmes doivent être maintenus à jour à la dernière version et constamment surveillés.
- Les schémas d'infrastructures, la documentation et les configurations doivent être à jour, contrôlés et disponibles pour contribuer à la résolution des incidents.

[5] BC/DR = Business Continuity / Disaster Recovery

8.5.1. ISOLEMENT DES INFRASTRUCTURES ET DES APPLICATIONS POUR PLUSIEURS UTILISATEURS

Computacenter conçoit que le fournisseur peut offrir ses services à plusieurs clients et, par conséquent, les normes suivantes doivent être respectées (à l'aide des techniques et organismes appropriés) :

- Un isolement logique des systèmes informatiques et des applications où les services sont exécutés.
- Tous les environnements virtuels dans lesquels sont fournis les services Computacenter doivent être isolés des autres clients du fournisseur grâce à des dispositifs de contrôle stricts.
- Les données doivent être séparées au niveau de l'architecture informatique conformément aux exigences en matière de l'architecture de sécurité des données.
- Tous les éléments nécessaires à la prestation des services à Computacenter (y compris les locaux ou l'infrastructure technique) sont, dans la mesure du possible, logiquement ou physiquement séparés des autres clients du fournisseur.

8.5.2. SÉPARATION DES ENVIRONNEMENTS DE PRODUCTION, DE TEST ET DE DÉVELOPPEMENT

- Le fournisseur garantira que pendant le développement et le maintien des services contractés, de la production, des environnements de tests et de développement, ainsi que des données associées à la production et aux tests sont séparés logiquement et physiquement.
- Les critères acceptables pour les nouveaux systèmes d'information, les mises à niveau et les nouvelles versions doivent être définis. Les tests appropriés doivent être réalisés sur le(s) système(s) au cours de la phase de développement et avant l'acceptation et déploiement sur l'environnement de production.
- Les droits d'accès sont contrôlés grâce aux regroupements appropriés et à la gestion des droits associés en vue d'assurer une séparation logique des données entre les différents clients.

8.5.3. GESTION DE LA DISPONIBILITÉ ; GESTION DE SAUVEGARDE

- Le fournisseur mettra en place un processus de gestion de la disponibilité approprié pour respecter les niveaux de service (dont ceux de la sécurité) accordés pour les services spécifiques délivrés à Computacenter ou à ses clients.
- Une gestion de sauvegarde appropriée sera mise en place pour assurer la disponibilité en cas d'urgence, et après tout incident majeur ou toute interruption de service. Ensuite, la gestion de reprise d'activité sera planifiée et testée.

8.5.4. GESTION DES ACTIFS ET DE LA CONFIGURATION

- Un registre des actifs doit être mis en place et conservé pour les services contractés avec Computacenter.
- Le fournisseur garantit que ces actifs informationnels ne soient pas partagés avec des tiers, à moins que ce ne soit en accord avec le processus de prestation des services contractés de Computacenter.
- Tous les actifs utilisés au cours de la prestation des services à Computacenter devraient être stockés de manière sécurisée et protégés contre tout accès, diffusion, modification, destruction ou interférence non autorisés.
- Toute information de Computacenter ou de ses clients doit être supprimée des dispositifs avant que ces derniers soient réutilisés à d'autres fins.

8.5.5. SUPERVISION DES OPÉRATIONS, GESTION DES JOURNAUX ET DES ÉVÉNEMENTS

- Un système automatique de reporting des événements devrait être disponible.
- Les journaux d'audits qui enregistrent l'activité des utilisateurs, les exceptions et les activités associées à la sécurité de l'information doivent être sauvegardés pendant une période convenue afin de faciliter les analyses et la surveillance du contrôle d'accès.
- Les contrôles techniques doivent être mis en place pour surveiller le système et garder une trace de toutes les activités associées au système de sécurité.
- Les journaux d'événements liés à la sécurité d'un des composants de l'infrastructure doivent être analysés et pris en charge.
- Le fournisseur doit avoir un processus de gestion des événements documenté, en place, et qui doit être testé pour détecter les cybermenaces pour les solutions et les services offerts.

8.5.6. GESTION DES CHANGEMENTS ET DE LA MISE EN PRODUCTION

- Le fournisseur se chargera de contrôler tous les changements des services contractés (à savoir uniquement les changements des processus business, des services informatiques, de l'application, de la plateforme ou de l'infrastructure, ou des changements physiques ou techniques des locaux) par le biais d'un processus officiel de gestion des changements.
- Lorsque les services contractés sont affectés, les modifications sont préalablement communiquées et approuvées par Computacenter.
- Toute mise en production de services et solutions ayant fait l'objet d'un changement ne peut avoir lieu qu'à partir de l'approbation d'une demande de changement et sur la base d'un processus formel de gestion de la mise en production du fournisseur.
- Toute livraison de logiciel en ligne ou distribution de logiciel automatique par le fournisseur doit respecter les politiques en matière de sécurité de l'information de Computacenter.

8.5.7. VULNÉRABILITÉ, GESTION DES CORRECTIFS ET TESTS D'INTRUSION

Le fournisseur doit avoir en place des processus de gestion des vulnérabilités et de gestion des correctifs efficaces, afin de réduire les risques résultant de l'exploitation des vulnérabilités techniques connues. Le fournisseur doit respecter la politique de gestion des vulnérabilités techniques de Computacenter.

9. GESTION DES COMPTES UTILISATEURS

9.1. ENREGISTREMENT, ANNULATION D'ENREGISTREMENT ET ÉVALUATION DES ACCÈS UTILISATEURS

Les fournisseurs seront chargés de gérer les comptes utilisateurs de son personnel conformément aux politiques d'identité, d'accès et de gestion des mots de passe et de bon usage de l'informatique de Computacenter. En particulier mais sans toutefois se limiter à ce qui suit ;

- Le fournisseur doit établir une procédure d'enregistrement et d'annulation de l'enregistrement de ses utilisateurs, tant pour les rôles fonctionnels comme pour les rôles d'administration ou privilégiés, qui doit être conservée et respectée lorsque le personnel du fournisseur accède aux environnements informatiques de Computacenter.
- Le fournisseur doit avoir un processus strict en place pour gérer les nouveaux arrivants/mutations/employés sortants de son équipe, impliqués dans la prestation de services à Computacenter.
    - Les comptes utilisateurs du personnel du fournisseur ayant muté ou quitté l'entreprise doivent être gérés de manière appropriée afin de minimiser tout accès non autorisé à l'environnement de Computacenter.
    - Lorsqu'un utilisateur enregistré quitte le fournisseur, ce dernier doit bloquer immédiatement le compte utilisateur associé à cette personne (dans un délai d'un jour ouvrable) et en informer l'équipe de gestion des accès de Computacenter.
- Le fournisseur doit examiner, tous les trimestres, la liste des identifiants enregistrés sur les systèmes Computacenter ainsi que les rôles et autorisations qui en découlent, en vue d'identifier de possibles écarts et d'harmoniser les résultats de ces examens avec les exigences de Computacenter.

9.2. CONTRÔLE D'ACCÈS, PRIVILÈGES ET APPROVISIONNEMENT LOGIQUE EN FONCTION DES RÔLES

Dans le cadre de la spécification des services, un plan sera convenu pour ce qui concerne les rôles et les responsabilités. Les rôles seront définis de manière que l'accès soit limité aux besoins commerciaux. Les rôles administrateurs dotés d'accès privilégiés seront également définis et accordés.

- Le fournisseur documentera les rôles privilégiés à mettre en place pour permettre au personnel du fournisseur d'accéder aux actifs informationnels de Computacenter.
- Le fournisseur sera chargé de fournir une solution pour l'enregistrement de tous les accès privilégiés. Ces journaux d'administration seront mis à disposition de Computacenter sur demande.

- Le fournisseur de services cloud indiquera quels sont les exigences concernant le contrôle d'accès à l'environnement cloud.
- Le fournisseur garantira un contrôle renforcé de tous les accès privilégiés et de la gestion des journaux pour toutes les activités privilégiées au niveau des systèmes, des bases de données, des briques logicielles et des applications business. Les activités exigeant un accès privilégié doivent être contrôlées par la gestion des journaux appropriée.

9.3. PROCÉDURES DE CONNEXION SÉCURISÉES

Le fournisseur s'assurera que les processus de connexion soient sécurisés, y compris par l'utilisation des standards industriels pour authentifier et autoriser (par ex. l'authentification multi-facteurs, pas d'utilisation des informations d'authentification utilisées en commun, l'expiration automatique) tous les comptes (standard ou privilégiés).

10. GESTION DES DISPOSITIFS MOBILES

- Le fournisseur veillera à adopter les mesures nécessaires pour se protéger des risques découlant de l'utilisation d'informatique mobile, du télétravail et des moyens de communication lorsqu'un collaborateur s'en sert pendant la prestation de services à Computacenter ou à ses clients.
- Le fournisseur et son personnel doivent respecter les politiques de Computacenter en matière de sécurité informatique.

11. GESTION DES INCIDENTS, REPORTING ET DIFFUSION

- Le fournisseur devra tenir à jour à tout moment les processus de gestion des incidents et des procédures qui comprennent les étapes à suivre pour la gestion des incidents majeurs ou des incidents de sécurité.
- Un processus de gestion des incidents documenté pour la sécurité physique et des données doit être mis en place, incluant la réponse aux incidents, l'escalade opérationnelle ou le changement de priorité et la résolution.
- Le personnel du fournisseur doit déclarer tout incident, faille de sécurité, ou événement touchant la sécurité au point de contact chez Computacenter et lui fournir toutes les données pertinentes.
    - Les incidents et les failles de sécurité ou les événements qui la touchent doivent être déclarés pas plus tard que 24 heures après avoir été détectés.
- En cas d'atteinte à la sécurité, pouvant faire l'objet de divulgation et d'autres obligations réglementaires de notification de la part de Computacenter, le fournisseur informera immédiatement son interlocuteur chez Computacenter.
- Les activités et incidents associés à la sécurité de l'information incluent, entre autres :
    - La perte du service, de l'équipement ou des installations
    - La défaillance ou la surcharge du système
    - Les erreurs humaines
    - La non-conformité aux politiques ou aux directives
    - Les infractions aux mesures de sécurité physique
    - Les modifications du système non maitrisés
    - Les défaillances du logiciel ou du matériel
    - Les accès non autorisés
    - Les infractions légales et aux règlements
    - Les logiciels malveillants
    - Les activités suspectes et anodines susceptibles d'un incident
- Le fournisseur doit mettre en place des processus de reporting pour tous les incidents majeurs et de sécurité pertinents de Computacenter, risquant d'impacter les exigences du contrat ou des conformités à la sécurité.
- Après la résolution de tout incident majeur ou de sécurité affectant les services délivrés, le fournisseur fournira les rapports des résultats et des changements initiés pour gérer toute faille ou vulnérabilité détectée en temps utile.
- Les deux entreprises agiront de bonne foi pour préserver les preuves de l'autre entreprise, et collaborerons entre elles et, si nécessaire, avec les autorités pertinentes si une enquête est menée.

12. PROTECTION CONTRE LES LOGICIELS MALVEILLANTS

- Le fournisseur doit avoir une solution antivirus en place sur tous les systèmes du fournisseur vulnérables aux risques d'infection par virus.
- La tierce partie devra utiliser toutes les mesures raisonnables pour détecter tout code caché ou toute information conçue pour avoir (ou qui aura) l'effet suivant :
    - Détruire, modifier, corrompre ou faciliter le vol de toute donnée de Computacenter

  - Désactiver ou bloquer tout logiciel, ou tout système du fournisseur ou de Computacenter
  - Utiliser des moyens d'accès non documentés ou non autorisés pour accéder aux données de Computacenter, ou aux systèmes informatiques de Computacenter ou du fournisseur
- Le fournisseur se chargera que l'outil de protection contre les logiciels malveillants :
  - soit une version actualisée et maintenue ;
  - soit actualisé avec des fichiers de définition ou des fichiers de signature au moins une fois par jour ;
  - offre des analyses à l'accès et sur demande en temps réel ;
  - analyse tout le contenu qui entre ou sorte de l'infrastructure informatique gérant l'information de Computacenter ;
  - soit capable de désinfecter, de mettre en quarantaine ou de supprimer les logiciels malveillants ;
  - fournisse des options de journalisation, d'alertes et de reporting ;
  - ne puisse être désactivé, reconfiguré ou bloqué par des utilisateurs non autorisés.
- La tierce partie devra assurer que le logiciel antivirus et les fichiers de définition antivirus soient mis à jour sur tous les systèmes du fournisseur conformément aux meilleures pratiques industrielles et aux recommandations pertinentes de l'éditeur du logiciel antivirus.
- Le fournisseur s'assurera que les dispositifs puissent détecter, isoler et détruire les codes malveillants présents.

13. CHIFFREMENT DES DONNÉES ET GESTION DU CHIFFREMENT

L'objectif des disposotifs cryptographiques (chiffrement des données, certificats numériques, signatures numériques) est d'assurer la confidentialité des données (pour en prévenir la diffusion non autorisée), de préserver l'intégrité des données (en prévenant ou en détectant toute modification non autorisée), et d'en assurer l'authenticité et la non-répudiation (en prouvant que l'émetteur de ces données est bien qui il prétend être).

- Le fournisseur doit garantir un chiffrement de données efficace sur les systèmes au repos. Le chiffrement sert à protéger les données en transit contenant des informations personnelles ou sensibles, ou tout autre type d'informations confidentielles comme stipulé par Computacenter, et doit donc être utilisé à ce propos.
- Aucun moyen de chiffrement ne doit pas être utilisé s'il n'offre pas un niveau de protection suffisamment élevé, à moins qu'il n'ait été autorisé par l'équipe de gestion de la sécurité de l'information de Computacenter.
- Le fournisseur doit planifier un processus de gestion des clés de bout en bout (détaillé) qui comprendra la génération de clés, leur utilisation, leur stockage et leur destruction (toujours de manière sécurisée).
  - Il est nécessaire de prendre en compte comment ces pratiques de gestion des clés peuvent faciliter la récupération des données chiffrées si jamais une clé est divulguée, détruite ou devient indisponible par inadvertance.
  - Le fournisseur doit assurer que l'accès aux clés de chiffrement soit sécurisé et ne soit accessible qu'au personnel autorisé. Les clés en soi doivent être physiquement en sécurité et au minimum deux administrateurs doivent y avoir accès.

14. GESTION DE LA CONTINUITÉ DES OPÉRATIONS ET PLANIFICATION DE LA REPRISE D'ACTIVITÉ APRÈS SINISTRE

Dans le cadre de la prestation de services à Computacenter ou à ses clients, le fournisseur doit respecter les normes indiquées ci-dessous en matière de continuité des opérations (Business Continuity ou BC) et de reprise d'activité après sinistre (Disaster Recovery ou DR) :

- Le fournisseur s'engage à participer dans la création et dans le maintien d'un plan d'urgence TIC (Technologies de l'information et des communications) aligné sur les normes ISO 22301 et ISO 27031. La première version du plan d'urgence et les éventuelles mises à jour doivent être présentées à Computacenter pour être planifiées par le Service Manager responsable (c'est à dire la personne de contact) du fournisseur. La validité de la version du document doit être confirmée par une approbation expresse et écrite de Computacenter.
- Le fournisseur doit garantir l'existence et la mise à jour des plans de gestion de continuité des opérations et de reprise d'activité après sinistre approuvés par l'équipe de Senior Management (y compris les éléments techniques et non techniques).
- Les plans BC/DR doivent fournir, de manière transparente, les solutions de contournement et les délais de rétablissement des services offerts à Computacenter ou à ses clients.
- Pendant la période BC/DR, le fournisseur doit établir des canaux de communication avec Computacenter.
- Tout le personnel du fournisseur impliqué dans la prestation du service doit connaître les plans BC/DR et leur responsabilité pendant la période BC/DR.
- Toutes les données de Computacenter disposent de fonctionnalités de sauvegarde et restauration qui sont mises en place, testées et planifiées régulièrement.

- Les ressources pour la reprise après sinistre et/ou du fournisseur doivent être documentées et mises à disposition de Computacenter sur demande.
- Le fournisseur s'engage également à participer activement dans les activités de Computacenter en cas d'urgence (si besoin), qui pourraient inclure les plans de continuité des opérations ou de reprise d'activité.

15. RÉSILIATION DE CONTRAT ; RETOUR D'INFORMATION ET TRAITEMENT DES ACTIFS

Une fois le contrat de service entre le fournisseur et Computacenter résilié, les points suivants doivent être respectés :

- Computacenter et le fournisseur doivent convenir d'un plan de gestion de sortie en temps voulu.
- Les plans de gestion de sortie doivent mentionner la fin des services délivrés à Computacenter, y compris les services basés sur le cloud, et/ou le transfert au fournisseur choisi par Computacenter sous la forme convenue.
- Le fournisseur doit rendre tous les actifs qui sont la propriété de Computacenter, et assurer la destruction de toute donnée dans l'environnement du fournisseur, comme spécifié dans le plan de gestion de sortie.

ANNEXE A

Les politiques de sécurité de l'information pertinentes de Computacenter sont énumérées ci-dessous. Le cas échéant, le fournisseur recevra les politiques pertinentes si nécessaire. Les fournisseurs qui, par exemple, travaillent sur les sites des clients pour le compte de Computacenter dans le cadre d'obligations contractuelles, seront tenus d'adhérer à ces politiques.

- Politique de Bon usage de l'informatique
- Politique d'Identité, d'accès et de gestion des mots de passe
- Politique de Gestion des vulnérabilités techniques
- Politique de Prévention de logiciels malveillants
- Politique de Sécurité informatique
- Politique de Sécurité des logiciels
- Politique de Sécurité des terminaux
- Politique de Sécurité des données informatiques
- Politique de l'Architecture de la sécurité informatique
- Politique de Gestion de la continuité des services informatiques
- Politique de Surveillance des environnements informatiques et du Journal des événements
- Politique de l'Infrastructure informatique technique (zones sécurisées)
- Politique d'Accès physique et de Sécurité du site