VNORMES EN MATIÈRE DE SECURITÉ INFORMATIQUE POUR LES FOURNISSEURS

VERSION ABREGÉE

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 peut y accéder.

1. 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 les auto-évaluations concernant l'information sur les risques et les contrôles de sécurité menées par le fournisseur.

Le personnel du fournisseur impliqué dans la livraison de produits et la prestation des services à Computacenter ou à ses clients doit respecter la politique de bon usage de l'informatique et de sécurité de l'information.

2. GESTION DU PERSONNEL (UTILISATEURS)

2.1. COMPTES D'UTILISATEUR

Il est possible que le personnel du fournisseur obtienne un compte utilisateur pour se connecter aux systèmes informatiques et aux applications de Computacenter. La gestion de ce type de comptes d'utilisateur doit respecter la politique de sécurité de l'information et d'identité, d'accès et de gestion des mots de passe de Computacenter.

- 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 devront être maintenus et respectés 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 utilisateur du personnel du fournisseur ayant muté ou quitté l'entreprise doivent être gérés de manière appropriée afin de minimiser l'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 Computacenter ainsi que les rôles et autorisations qui en découlent, en vue d'identifier les possibles écarts et d'harmoniser les résultats de ces examens avec les exigences de Computacenter.
- Le personnel du fournisseur ne peut utiliser le(s) compte(s) d'utilisateur fourni(s) après la fin du contrat avec Computacenter ou avec ses clients.

2.2. UTILISATION DU SYSTÈME DE MESSAGERIE ÉLECTRONIQUE

Des adresses électroniques peuvent être fournies au personnel du fournisseur de bonne foi à des fins professionnelles de Computacenter et conformément à la politique de bon usage de l'informatique de Computacenter. Chaque individu est dans l'obligeance de lire et de signer la « Déclaration d'engagement pour les externes » avant que Computacenter n'accorde l'accès à cette adresse électronique.

2.3. CONTROLE D'IDENTITÉ, VÉRIFICATION ET FILTRAGE

Le fournisseur doit assurer la conformité à la politique de bon usage de l'informatique de Computacenter et aux politiques au niveau local supplémentaires/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.

2.4. CONSIGNES POUR LE PERSONNEL DU FOURNISSEUR ET COMPORTEMENT EXIGÉ

Le personnel du fournisseur doit se conformer aux politiques d'accès physique et de sécurité du site. Le fournisseur doit assurer que son personnel de service (y compris les collaborateurs ou agents des sous-traitants) n'utilise les sites, l'équipement ou le logiciel de Computacenter :

- pour transmettre, publier ou distribuer du matériel diffamatoire ou susceptible d'être considéré offensif, abusif, obscène ou menaçant,
- de manière à constituer une atteinte aux droits de toute personne ou entreprise (comprenant, entre autres, les droits d'auteur ou de confidentialité),
- à des fins personnelles,

et que le personnel soit dûment informé des exigences découlant des politiques en matière de sécurité de l'information de Computacenter et respecte ces normes.

Une conduite inacceptable identifiée pendant l'exercice des activités peut signifier que cet utilisateur soit exclu du site et dénoncé auprès de l'équipe de direction du fournisseur. Un processus disciplinaire formel doit être suivi pour les employés du fournisseur ayant menacé la sécurité de l'entreprise.

2.5. FORMATION DU PERSONNEL DU FOURNISSEUR

Le fournisseur garantit que le personnel travaillant pour Computacenter ou ses clients ait suivi la formation de sensibilisation à la sécurité de l'information appropriée. Ce type de formation doit être fournie comme partie intégrante de l'intégration d'un nouvel arrivé, et comme formation de mise à niveau pour le personnel existant.

3. GESTION DE L'ÉQUIPEMENT INFORMATIQUE

3.1. UTILISATION DE L'ÉQUIPEMENT INFORMATIQUE ET DES BIENS

Il est possible que le personnel du fournisseur obtienne de l'équipement informatique ou d'autres produits de Computacenter. Comme par exemple, des jetons d'authentification à deux facteurs, des badges ou cartes avec photos, des ordinateurs personnels et des ordinateurs portables. Il est strictement interdit d'utiliser les supports amovibles (comme les lecteurs USB chiffrés), à moins que Computacenter ne l'autorise par écrit. Le personnel du fournisseur doit rendre tout l'équipement à Computacenter sur demande. Il doit également informer immédiatement le Service Desk informatique interne de Computacenter en cas de perte ou de vol d'équipement. Le Service Desk informatique interne est joignable 24h/24, 7j/7, 365 jours par an aux numéros suivants :

- +44 (0)1707 631111 (EN)
- +49 2273 597 7777 (DE)
- +33 148 176 99 (FR)

En cas de perte ou de vol de matériel du client fourni au personnel du fournisseur, le parrain ou point de contact de Computacenter doit être informé immédiatement, afin d'assurer que la situation soit gérée de manière appropriée et que le client soit tenu au courant. Les Service Managers ou les points de contact de Computacenter pertinents sont les seuls qui devraient informer le client.

Tout équipement informatique fourni par Computacenter (par ex. ordinateur portable, PC, téléphone portable) contenant des données de Computacenter ou de ses clients doit être protégé contre tout accès non autorisé, abus ou corruption pendant son transport au-delà des limites physiques du fournisseur et dans les limites du raisonnable. L'équipement informatique, les supports ou les données ne doivent pas sortir des locaux des sous-traitants sans autorisation.

3.2. L'UTILISATION DE L'ÉQUIPEMENT INFORMATIQUE DONT COMPUTACENTER N'EST PAS PROPRIÉTAIRE

L'équipement informatique dont Computacenter n'est pas propriétaire (par ex. dont la propriété est privée et non celle de l'entreprise) ne peut être utilisé dans la prestation de services à Computacenter ni à ses clients. Ceci comprend l'utilisation de smartphones, tablettes et PDA privés pour copier et/ou enregistrer l'information.

3.3. ACCÈS À DISTANCE

Si le fournisseur exige un accès à distance à l'environnement informatique de Computacenter, il doit :

- y accéder uniquement en utilisant les comptes d'utilisateurs fournis par Computacenter,
- Accès par le biais d'un modèle d'accès à distance de type "concierge[1]", par partage d'écran avec un employé de Computacenter permettant uniquement l'accès au système pendant la période requise.
- y accéder uniquement en utilisant les systèmes d'accès à distance[2] disponibles et s'en tenir au processus prévu,
- n'autoriser le compte utilisateur désigné que pour les raisons choisies (qui doivent être enregistrées dans des rapports d'incidents/demandes/modifications),
- éviter à tout prix de copier (sur papier ou électroniquement) toute information ou donnée sans l'autorisation explicite de Computacenter.

[1] 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.

[2] Les systèmes d'accès à distance (Remote Access System ou RAS) - solutions technologiques du centre informatique pour obtenir un accès à distance.

4. GESTION DES INCIDENTS, REPORTING ET DIFFUSION

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 en temps opportun, pas plus de 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.

Si le fournisseur observe ou soupçonne une atteinte à la confidentialité d'un compte utilisateur qui lui a été fourni par Computacenter, il est tenu d'en informer Computacenter immédiatement.

ANNEXE

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 et de Sécurité de l'information
- Politique de Sécurité de l'information et d'identité, d'accès et de gestion des mots de passe
- Politique d'Accès physique et de Sécurité du site