

Politique de réponse aux incidents de sécurité informatique

Rév. 2023

But

Cette politique définit les exigences en matière de déclaration et de réponse aux incidents liés aux systèmes d'information et aux opérations de Appligogiques.

Portée

Cette politique s'applique à tous les employés et partenaires des entités de Appligogiques, y compris, sans s'y limiter, les unités commerciales et les filiales.

Politique

Organisation du programme

Plans d'intervention en cas d'urgence informatique

La direction de Appligogiques doit élaborer, mettre à jour périodiquement et tester régulièrement des plans d'intervention d'urgence qui prévoient le maintien en fonctionnement des systèmes informatiques et de communication critiques en cas d'interruption ou de dégradation du service.

Contenu du plan de réponse aux incidents

Le plan d'intervention en cas d'incident de Appligogiques doit inclure les rôles, les responsabilités et les stratégies de communication en cas de compromission, y compris la notification des partenaires externes pertinents. Les domaines spécifiques abordés dans le plan comprennent:

- Procédures spécifiques de réponse aux incidents.
- Procédures de reprise et de continuité des activités.
- Processus de sauvegarde des données.
- Analyse des exigences légales pour le signalement des compromissions.
- Identification et couverture de tous les composants critiques du système.

- Référence ou inclusion des procédures de réponse aux incidents de partenaires externes pertinents, par exemple, émetteurs de cartes de paiement, fournisseurs.

Équipe de réponse aux incidents de sécurité

Équipe de réponse aux incidents de sécurité

La direction de Appligogiques doit organiser et maintenir une équipe interne de réponse aux incidents de sécurité ou être en contact avec un tiers proposant des services de réponse en matière de sécurité, capable de fournir une notification accélérée des problèmes, des services de contrôle des dommages et de correction des problèmes en cas d'urgences liées à l'informatique, telles que des infestations virales et des intrusions de pirates informatiques.

Disponibilité de l'équipe d'intervention en cas d'incident informatique

L'équipe de réponse aux incidents de sécurité de Appligogiques doit toujours être disponible pour répondre aux alertes comprenant, sans s'y limiter, des preuves d'activité non autorisée, la détection de points d'accès sans fil non autorisés, des alertes critiques de détection d'intrusion et des signalements de modifications non autorisées de systèmes critiques ou de fichiers de contenu.

Rôles et responsabilités

Responsabilités de la gestion des incidents

Les personnes responsables de la gestion des incidents de sécurité des systèmes d'information doivent être clairement définies par le CTO. Ces personnes doivent se voir conférer l'autorité nécessaire pour définir les procédures et méthodologies qui seront utilisées pour gérer les incidents de sécurité spécifiques.

Personne de contact désignée pour toutes les catastrophes et les événements de sécurité

Sauf s'ils sont expressément reconnus comme porte-parole autorisés de Appligogiques, aucun employé ne peut parler à la presse ou à

toute autre partie externe de l'état actuel d'une catastrophe, d'une situation d'urgence ou d'un événement de sécurité récemment vécu.

Fournir des informations dans le cadre de procédures judiciaires

Il est interdit aux employés de fournir des dossiers de Appligogiques, ou des copies de ceux-ci, à des tiers extérieurs à Appligogiques ou à des fonctionnaires gouvernementaux, que ce soit en réponse à une assignation à comparaître ou autrement, à moins d'avoir obtenu au préalable l'autorisation de la direction de Appligogiques. De même, il est interdit aux employés de témoigner de faits dont ils ont eu connaissance dans l'exercice de leurs fonctions officielles chez Appligogiques, à moins d'avoir obtenu au préalable l'autorisation de la direction de Appligogiques.

Réponse aux incidents et récupération

Procédures de réponse aux intrusions

Le service informatique doit documenter et réviser périodiquement les procédures de réponse aux intrusions. Ces procédures doivent inclure la séquence d'actions que le personnel doit suivre en cas de suspicion d'intrusion dans le système d'information, qui a l'autorité pour effectuer quelles actions en réponse, et quels sont les ressources disponibles pour aider à la réponse. Tout le personnel devant suivre ces procédures doit être formé périodiquement et familiarisé avec ces procédures.

Résolution des problèmes de sécurité de l'information

Tous les problèmes de sécurité de l'information doivent être traités avec la participation et la coopération du personnel chargé de la sécurité de l'information, de la direction de Appligogiques ou d'autres personnes autorisées par la direction de Appligogiques.

Modifications de sécurité après compromission du système

Chaque fois qu'un système a été compromis, ou est suspecté d'avoir été compromis par une partie non autorisée, les administrateurs système doivent immédiatement recharger une version fiable du système d'exploitation ainsi que tous les logiciels liés à la sécurité, et toutes les modifications récentes des privilèges utilisateur et système doivent être examinées pour détecter d'éventuelles modifications non autorisées.

Intrusions système suspectées

Chaque fois qu'un système est suspecté d'avoir été compromis, l'ordinateur concerné doit être immédiatement déconnecté de tous les réseaux, et les procédures prédéterminées doivent être suivies pour s'assurer que le système est exempt de compromission avant de le

reconnecter au réseau.

Problèmes d'accès non autorisé

Chaque fois qu'un accès non autorisé au système est suspecté ou avéré, le personnel de Appligogiques doit prendre des mesures immédiates pour mettre fin à cet accès ou demander l'assistance du CTO.

Enquêtes internes Confidentialité des informations

Jusqu'à ce que des accusations soient portées ou des mesures disciplinaires prises, toutes les enquêtes sur des allégations de comportement criminel ou abusif doivent être maintenues strictement confidentielles afin de préserver la réputation de la partie suspectée.

Participation aux procédures judiciaires

Tout employé de Appligogiques convoqué par assignation à comparaître ou de toute autre manière devant un conseil judiciaire ou un organisme gouvernemental doit immédiatement notifier par écrit le conseiller juridique en chef de l'appel.

Surveillance des événements

Surveillance et enregistrement de l'utilisation des ressources informatiques partagées

L'utilisation de toutes les ressources informatiques partagées de Appligogiques utilisées pour les activités de production doit être surveillée en continu et enregistrée. Ces données d'historique d'utilisation doivent ensuite être fournies en temps réel aux systèmes d'alerte de sécurité désignés par le service informatique (systèmes de détection d'intrusion, systèmes de détection de virus, systèmes de détection de spam, etc.).

Signalement des événements de sécurité de l'information

Rapports d'incidents

Tous les incidents présumés de sécurité de l'information doivent être signalés aussi rapidement que possible via les canaux internes approuvés de Appligogiques.

Système d'alerte de sécurité de l'information

Le département de sécurité doit établir, maintenir et tester périodiquement un système de communication permettant aux employés de signaler rapidement aux membres du personnel appropriés tout problème présumé de sécurité de l'information.

Alternatives de signalement des violations et des problèmes

Les employés de Appligogiques doivent signaler immédiatement tous les problèmes, vulnérabilités et incidents présumés liés à la sécurité de l'information à leur responsable hiérarchique.

Protection contre les violations et les rapports de problèmes

Appligogiques protégera les employés qui signalent de bonne foi ce qu'ils estiment être une violation des lois ou des réglementations, ou des conditions pouvant mettre en danger la santé ou la sécurité des autres employés. Cela signifie que ces employés ne seront pas licenciés, menacés ou discriminés parce qu'ils dénoncent ce qu'ils considèrent comme un acte répréhensible ou une situation dangereuse.

Identité de rapport de violation et de problème

Les employés qui signalent au service informatique un problème de sécurité, une vulnérabilité ou une situation contraire à l'éthique au sein de Appligogiques peuvent, à leur seule discrétion, avoir leur identité strictement confidentielle. Cela signifie que l'identité du lanceur d'alerte ne sera pas révélée à son supérieur hiérarchique, aux autres membres de l'équipe de direction ni aux autres employés de Appligogiques qui ne sont pas directement impliqués dans la réception du signalement.

Événements à signaler

Dommages et pertes de systèmes hors site

Les employés doivent signaler immédiatement à leur responsable tout dommage ou perte de matériel informatique, de logiciel ou d'informations de Appligogiques qui leur ont été confiés.

Alertes et avertissements système

Les utilisateurs doivent signaler promptement toutes les alertes de sécurité, les avertissements, les vulnérabilités suspectées et similaires au service d'assistance des systèmes d'information. Les utilisateurs sont interdits d'utiliser les systèmes de Appligogiques pour transmettre de telles informations à d'autres utilisateurs, qu'ils soient internes ou externes à Appligogiques.

Activité non autorisée

Les utilisateurs des systèmes d'information de Appligogiques doivent signaler immédiatement au responsable du service informatique toute perte non autorisée ou modification des données de production informatisées. Toute utilisation douteuse des fichiers, des bases de données ou des réseaux de communication doit également être signalée immédiatement au même responsable.

Demandes inattendues d'informations de connexion

Mis à part les écrans de connexion réguliers et attendus de Appligogiques, les utilisateurs doivent se méfier de toutes les fenêtres contextuelles, sites web, messages instantanés et autres demandes de nom d'utilisateur et de mot de passe Appligogiques. Les utilisateurs qui rencontrent ces demandes doivent s'abstenir de fournir leur nom d'utilisateur et leur mot de passe Appligogiques, et signaler rapidement les circonstances au service d'assistance.

Périphériques d'accès manquants

Les badges d'identification et les cartes d'accès physique qui ont été perdus, volés ou dont la perte est suspectée doivent être signalés immédiatement au service informatique. De même, tous les ordinateurs ou jetons d'accès aux systèmes de communication (cartes à

puce avec mots de passe dynamiques, cartes de crédit téléphonique, etc.) qui ont été perdus, volés ou dont la perte est suspectée doivent être signalés immédiatement.

Divulgation involontaire d'informations sensibles

Les divulgations non intentionnelles d'informations sensibles de Appligogiques sont des problèmes graves et doivent être immédiatement signalées à la fois au conseiller juridique en chef et au responsable du service informatique. Un tel signalement doit avoir lieu dès que la divulgation est connue, ou dès qu'il existe des motifs raisonnables de croire qu'une divulgation a eu lieu.

Dysfonctionnements logiciels

Tous les dysfonctionnements apparents du logiciel doivent être signalés immédiatement à la direction ou au fournisseur de services du système d'information.

Points d'accès sans fil non autorisés

Si un point d'accès sans fil non autorisé est détecté sur le réseau Appligogiques, l'équipe d'intervention en cas d'incident informatique doit être informée.

Rapports à des tiers

Signalement de violation externe

À moins d'être tenus par la loi ou la réglementation de signaler les violations de sécurité de l'information aux autorités externes, la direction supérieure, en collaboration avec des représentants du service juridique et du service informatique, doit évaluer les avantages et les inconvénients de la divulgation externe avant de signaler ces violations.

Signalement des failles de sécurité suspectées à des tiers

Si un problème de sécurité des systèmes d'information vérifiable, ou un problème présumé mais probable de sécurité de l'information, a entraîné l'exposition d'informations privées ou confidentielles de tiers à des personnes non autorisées, ces tiers doivent être informés immédiatement de la situation.

Perte ou divulgation d'informations sensibles

Si des informations sensibles sont perdues, divulguées à des parties non autorisées, ou si l'on soupçonne qu'elles ont été perdues ou divulguées à des parties non autorisées, leur propriétaire ainsi que le service informatique doivent être immédiatement informés.

Exploitation des vulnérabilités du système et données sur les victimes

Le personnel de Appligogiques ne doit pas divulguer publiquement des informations sur les personnes, les organisations ou les systèmes spécifiques qui ont été endommagés par des

crimes informatiques et des abus informatiques. De même, les méthodes spécifiques utilisées pour exploiter certaines vulnérabilités du système ne doivent pas être divulguées publiquement.

Divulgation de la vulnérabilité des fournisseurs

Si les employés de Appligogiques découvrent une vulnérabilité sérieuse dans un système d'information, et que cette vulnérabilité peut être directement attribuée à une faiblesse dans le matériel et/ou les logiciels d'un certain fournisseur, ce fournisseur doit être rapidement et confidentiellement informé du problème.

Contact avec les autorités

Contact avec la communauté de la justice pénale

Le personnel technique des systèmes d'information ne doit pas contacter la police ou d'autres membres du système judiciaire au sujet de problèmes de systèmes d'information, à moins d'avoir reçu l'autorisation de la direction de Appligogiques.

Demandes d'application de la loi

Même si la partie demanderesse prétend être un membre des forces de l'ordre, les employés de Appligogiques ne doivent divulguer aucune information interne de Appligogiques par le biais d'un quelconque mécanisme de communication, à moins d'avoir établi l'authenticité de l'identité de la personne et la légitimité de la demande.

Contacter les forces de l'ordre

Chaque décision concernant l'implication des forces de l'ordre dans les incidents ou problèmes de sécurité de l'information doit être prise par un associé senior de Appligogiques. De même, chaque contact informant les forces de l'ordre d'un incident ou d'un problème de

sécurité de l'information doit être initié par le responsable du service informatique.

Demandes de coopération aux enquêtes

Les employés de Appligogiques doivent signaler immédiatement toute demande de participation à une enquête sur la sécurité de l'information au conseiller juridique en chef. Toute forme de coopération avec la partie demanderesse est interdite jusqu'à ce que le conseiller juridique en chef détermine que la participation est légale, peu susceptible de causer des problèmes pour Appligogiques et demandée par une partie autorisée.

Gestion des violations de données

appligogiques

Plan d'intervention en cas de violation de données requis

La direction de Appligogiques doit préparer, tester et mettre à jour annuellement un plan de réponse aux violations de données qui aborde les politiques et les procédures de réponse en cas de violation des données sensibles des clients.

Examen des incidents

Évolution du plan de réponse aux incidents - Leçons apprises

Le plan d'intervention en cas d'incident doit être mis à jour pour refléter les enseignements tirés des incidents réels.

Évolution du plan de réponse aux incidents - Développements de l'industrie

Le plan d'intervention en cas d'incident doit être mis à jour pour refléter les évolutions de l'industrie.

Analyse des violations et des problèmes

Le département informatique doit préparer une analyse annuelle des problèmes de sécurité de l'information signalés et des violations.

Collecte de preuves

Preuve de crime ou d'abus informatique

Pour fournir des preuves pour une enquête, des poursuites judiciaires et des mesures disciplinaires, certaines informations doivent être immédiatement collectées dès lors qu'un crime informatique ou un abus est suspecté. Les informations à collecter immédiatement comprennent la configuration système actuelle ainsi que des copies de sauvegarde de tous les fichiers potentiellement impliqués.

Stockage des preuves

Les informations pertinentes pour l'enquête informatique doivent ensuite être stockées de manière sécurisée hors ligne jusqu'à ce qu'elles soient remises à une autre personne autorisée ou que le conseiller juridique en chef détermine que Appligogiques n'aura plus besoin des informations.

Sources de preuves numériques

Pour chaque système informatique de production, le service informatique doit identifier les sources de preuves numériques qui pourraient raisonnablement être utilisées dans une affaire judiciaire. Ces sources de preuves doivent ensuite faire l'objet d'un processus

normalisé de collecte, de conservation et de destruction comparable à celui utilisé pour les documents essentiels.

Responsabilité de la production de preuves électroniques

Appligogiques désignera une seule personne responsable de coordonner la découverte et la présentation des preuves électroniques qui pourraient être nécessaires pour soutenir un litige.

Classement des informations

Les données de Appligogiques pouvant être considérées comme des preuves électroniques doivent être classifiées comme CONFIDENTIELLES et ne doivent être consultées que par les représentants autorisés de l'équipe d'intervention en cas d'incident de sécurité ou par des tiers approuvés impliqués dans l'enquête.

Enquête et judiciaire

Enquête sur la criminalité informatique

Chaque fois que les preuves montrent clairement que Appligogiques a été victime d'un crime informatique ou de communication, une enquête approfondie doit être réalisée. Cette enquête doit fournir suffisamment d'informations pour que la direction puisse prendre des mesures afin de s'assurer que (1) de tels incidents ne se reproduiront pas à l'avenir et (2) des mesures de sécurité efficaces ont été rétablies.

Processus d'analyse judiciaire

Toute analyse ou enquête utilisant des supports de stockage de données contenant des informations qui pourraient à un moment donné devenir des éléments de preuve importants lors d'un procès pour crime informatique ou abus informatique doit être effectuée à l'aide d'une copie plutôt que de la version originale. Cela contribuera à

prévenir toute modification imprévue des informations d'origine.

Rapports d'état d'enquête

Le statut des enquêtes sur la sécurité de l'information doit être communiqué à la direction uniquement par l'enquêteur principal ou le représentant de la direction de l'équipe d'enquête.

Informations sur les enquêtes sur les délits informatiques

Toutes les preuves, idées et hypothèses concernant les crimes informatiques subis par Appligogiques, y compris les méthodes d'attaque possibles et les intentions des auteurs, doivent être communiquées au conseiller juridique en chef et considérées comme des informations restreintes et confidentielles protégées par la loi.

Enquêtes de sécurité de l'information

Toutes les enquêtes internes de Appligogiques sur les incidents, violations et problèmes de sécurité de l'information doivent être menées par du personnel formé et autorisé par le responsable du service informatique.

Équipes d'enquête sur la sécurité de l'information

Toute personne qui connaît personnellement les suspects, ou qui entretient des relations amicales avec eux, pour des raisons de conflit d'intérêts, est exclue de la participation à une équipe d'enquête sur les incidents de sécurité de l'information.

Détails des enquêtes sur les intrusions

Les détails concernant les enquêtes sur les intrusions dans les systèmes d'information en cours ne doivent pas être envoyés par courrier électronique. De même, pour empêcher que de telles informations ne tombent entre les mains des intrus, les fichiers décrivant une enquête en cours ne doivent pas être stockés sur des systèmes potentiellement compromis, ni nulle part sur un réseau associé où ils pourraient raisonnablement être consultés par des intrus.

Infractions

Toute violation de cette politique peut entraîner des mesures disciplinaires, y compris le licenciement. Appligogiques se réserve le droit de signaler aux autorités compétentes toute activité illégale et de coopérer à toute enquête sur une telle activité. Appligogiques ne considère pas les comportements en violation de cette politique comme relevant du cours normal des activités d'un employé ou d'un partenaire, ni comme une conséquence directe de l'exercice de leurs fonctions. En conséquence, dans la mesure permise par la loi, Appligogiques se réserve le droit de ne pas défendre ni de payer les dommages-intérêts accordés à des employés ou des partenaires résultant

d'une violation de cette politique.

Définitions

- Partenaire : Toute personne non employée de Appligogiques qui est liée contractuellement à fournir une forme de service à Appligogiques.

- Mot de passe : Une chaîne arbitraire de caractères choisie par un utilisateur et utilisée pour authentifier l'utilisateur lorsqu'il tente de se connecter, afin de prévenir l'accès non autorisé à son compte.

- Administrateur système : Un employé ou un partenaire chargé de la gestion d'un environnement informatique multi-utilisateurs de Appligogiques. Les responsabilités de l'administrateur système comprennent généralement l'installation et la configuration du

matériel et des logiciels du système, la création et la gestion des comptes utilisateurs, la mise à niveau des logiciels ainsi que les tâches de sauvegarde et de récupération.

- Utilisateur : Tout employé ou partenaire de Appligogiques autorisé à accéder à une ressource électronique de Appligogiques.

Références

- ISO/CEI 27002 : 16.0 Gestion des incidents de sécurité de l'information
- NIST : Réponse aux incidents (IR)
- HIPAA : Procédures d'incident de sécurité 164.308(a)(6)
- PCI-DSS : Plan de réponse aux incidents 12.10

appligogiques

ANNEXE : RAPPORT SOMMAIRE D'INCIDENT

TYPE D'INCIDENT	
DATE D'ORIGINE DE L'INCIDENT	
DATE DE DETECTION DE L'INCIDENT	
PAR QUI L'INCIDENT A ÉTÉ DÉTECTÉ	
COMMENT L'INCIDENT A-T-IL ÉTÉ DÉTECTÉ	
PORTÉE DE L'INCIDENT (SYSTÈMES AFFECTÉS)	
DATE INCIDENT CORRIGÉ	
TYPES D'ACTIONS CORRECTIVES (FORMATION,	

Résumé des symptômes de l'incident

Résumé du type et de la portée de

l'incident Résumé des actions correctives

Synthèse des processus d'atténuation et communication interne

Journal des communications

(Joindre des brouillons pour les communications écrites, un synopsis pour la communication verbale)

DATE DE COMMUNICATIO	TYPE DE COMMUNICATIO	BÉNÉFICIAIRE(S)	BUT

[DATE]

Chers clients,

Nous vous écrivons pour vous informer d'un incident qui s'est produit au sein de XXXXXXX. Cet incident a entraîné la compromission de données d'élèves/personnel/etc. par une entité externe. Notre équipe d'intervention en cas d'incident a agi rapidement pour évaluer et atténuer la situation.

À l'heure actuelle, nous sommes en mesure de vous fournir les informations suivantes :

[insérer une brève description de la violation ou de la divulgation non autorisée, les dates de l'incident et la date de découverte ; une description des types d'informations personnelles identifiables affectées ; une estimation du nombre d'enregistrements affectés ; une brève description ou un plan pour mener l'enquête]

Sachez que XXXXXXX s'engage à protéger et sécuriser les données éducatives. Notre équipe dispose d'une formation approfondie en matière de sécurité et de confidentialité des données, et nos systèmes sont dotés de nombreux mécanismes de protection de vos données. Notre équipe collabore avec un groupe d'experts pour examiner l'incident et mettre en place des mesures appropriées afin de prévenir de tels incidents à l'avenir.

N'hésitez pas à contacter XXXXXXX pour toute question concernant cet

incident et notre réponse. Cordialement,

XXXXXXX