

POLITIQUE DE SÉCURITÉ DU SYSTÈME D'INFORMATION

Historique des révisions

Dernière mise à jour	Décembre 2020
----------------------	---------------

Modifier par	
--------------	--

GROUPE MEDIA CONTACT SA



Avenue Dorothée LIMA, rue 11010
Gbegamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

Tableau des matières

1.Principes de protection des donn	9
2.Dispositions générale	99
3.Traitement légal, équitable et transparent	1010
4.Buts légitimes	1010
5.Accuracy	1111
6.Archivage / Déménagement	1111
7.Sécurité	1111
8.Violation	1211
9.Énoncé de politique	1414
10.But	1414
11.Portée	1414
12.Politique	1515
Application de la Politique	1515
Normes de sécurité des contacts avec les médias debaseline Group	15 15
Sécurité physique	1515
Zones sécurisées debase	16 16
Zones sécurisées améliorées	16 16
Répondre aux atteintes à la sécurité de toute zone sécurisée	1717
Menaces sur les biens d'information	1717
Sécurité des informations sur papier	1718
Équipement TIC Sécurité	1818
Câblage Sécurité	19 19
Informations sur l'entretien de l'équipement	19 19
Sécurité de l'équipement hors site	2020
Élimination ou réutilisation sécurisée de l'équipement	2020
Livraison et réception de l'équipement dans le Groupe Media Contact	2020
13.Vérification régulière	2121
14.Application des politiques	2121
15.Gouvernance des politiques	2121
16.Examen et révision	2222

GRUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112



17.Énoncé de politique	2424
18.Définitions.....	2424
Réseau vaste (WAN).....	2424
Réseau 19.Corporate	2424
20.Objectifs politiques.....	2525
21.Application	2626
22.Directives politiques	2626
Lignes directrices générales en matière desécurité réseau	26 26
Identification/Authentification	2828
Contrôles d'accès/autorisation	2828
LAN	2828
WAN	2828 (en)
23.Accès à distance	2929
24.Pare-feu	3030
25.Fournisseurs de services de télécommunications	3030
26.Entrepreneurs.....	3030
27.Sécurité physique et environnementale	3131
Synchronisation 28.Time.....	3232
29.Révocation/résiliation des privilèges wan.....	3232
30.Change Control	3333
31.Mécanismes de gestion des risques de sécurité et planification	3333
32.Certification et accréditation	3535
33.Security Journaux et enregistrements	3635
34.Rapports et enquêtes sur les incidents	3636
35.Information/Documentation de sécurité	3736
36.Surveillance/Surveillance et protection de la vieprivée.....	37 37
37.Formation en sécurité	3838
38.Responsabilités	3838
Directeurs généraux (GM)	3838
Chef del'information	3838
Coordonnateur des politiques de sécurité	3838
Comité desécurité.....	38 38

GRUPE MEDIA CONTACT SA



Avenue Dorothee LIMA, rue 11010
Gbegamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112





Sécurité des clients	3939
Organisation cliente	39 39
Entité externe	3939
Gestionnaires et personnel délégué	3939
Organisations hébergeant wan facilities	3939
39.Surveillance (de la politique de sécurité de l'WAN)	3939
Directeur général	3939
Coordonnateur des politiques de sécurité	4039
Comité de sécurité	4040
Gestion des services d'infrastructure (ISM)	4040
Agent de sécurité des clients ou désigné	40 40
40.Demandes de renseignements	4040
41.Glossaire	4040
Contrôle d'accès	40 40
Accréditation	4141
Authentification	4141
Bastion Hôte	4141
Certification	4141
Organisation cliente	41 41
Confidentialité	4141
Entrepreneur	4141
Réseau d'entreprise	41 41
Soins dus	4141
Diligence raisonnable	4241
Entité externe	4242
Pare-feu	4242
Intégrité	4242
Modem (Modular-Demodulator)	4242
Moniteur	4242
Profil de sécurité	42 42
Comité de sécurité	4242
Incident de	42 sécurité 42

GROUPE MEDIA CONTACT SA



Avenue Dorothee LIMA, rue 11010
Gbegamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112



Gestion des risques de	42	sécurité 42
Fournisseur de	43	services 43
Synchronisation du temps.....	43	43
Menace.....	43	43
Évaluation des menaces et des.....	43	risques 43
Réseau nontrusted	43	43
42.Énoncé de politique	45	45
43.But.....	45	45
44.Portée.....	45	45
45.Définition	45	45
46.Risques.....	45	45
Acquisition 47.Software	46	46
48.Enregistrement logiciel.....	46	46
49.Applications.....	47	47
Installation 50.Software	48	48
51.Application et développement de logiciels.....	48	48
équipement informatique 52.Personal.....	49	49
53.Software Misuse	49	49
54.Conformité aux politiques	49	49
55.Gouvernance des politiques.....	50	50
56.Examen et révision	50	50
Messages 57.Key	51	51
58.Énoncé de politique	53	53
Responsabilité des services d'information(SI)	53	53
S'attaque aux risquesmajeurs	53	53
59.Renseignements applicables.....	53	53
60.Procédures.....	54	54
Contrôled'accès	54	54
Contrôles d'accès ausystème.....	54	54
Décisions d'octroid'accès.....	54	54
61.Classification de l'information.....	54	54
Renseignements sur les propriétaires et laproduction.....	54	54

GROUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbegamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 **+229 95 17 00 16**
contact@groupmediacontact.com

 **RCCM N° : RB/COT/13B 10291**
IFU N° : 3201300930112



Restreint	5555
Confidentiel	5555
Public	5555
Décisions relatives aux propriétaires et à	55l'accès 55
62.Object Réutilisation et élimination	5555
63.Sécurité physique	5656
Accès au centre de	56données 56
Accès aux	56installations 56
Considérations spéciales pour l'information	56restreinte 56
Logiciel de cryptage	56des données 56
64.Transfert d'informations	5656
Transmission au-dessus des	56réseaux 56
Transfert vers un autre ordinateur	5757
65.Software Security	5757
Stockage sécurisé de l'objet et du code source	5757
Test	5757
Sauvegardes	5757
66.Gestion clé	5757
Protection des clés	5757
Procédures	5757
Sauvegarde des clés	5858
67. Vue d'ensemble	6060
68. Portée	6060
69. Politique	6060
Création de mot de passe	60 60
Mot de passe Vieillessement	60 60
Protection par mot de passe	60 60
Exécution	6161
70.But	6363
71.Portée	6363
72.Accès tiers	6363
Directeur	6363

GROUPE MEDIA CONTACT SA



Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112



MEDIA CONTACT

The offshore company

Pratiques.....	6363
Exigences de tiers	6363
Exigences internes.....	6565

GRUPE MEDIA CONTACT SA



Avenue Dorothée LIMA, rue 11010
Gbgamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112



Groupe Media Contact



www.groupmediacontact.com

I. POLITIQUE DE PROTECTION DES DONNÉES

Historique des révisions

Dernière mise à jour	Décembre 2020
-------------------------	---------------

GRUPE MEDIA CONTACT SA

 Avenue Dorothée LIMA, rue 11010
Gbegamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

1. Protection des données Principles

Group Media Contact s'engage à traiter les données en vertu de ses responsabilités en vertu des lois sur la confidentialité des données. Les lois sur la protection de la vie privée exigent fondamentalement que les données personnelles soient :

- a) Traité légalement, équitablement et de manière transparente concernant les individus.
- b) Recueillies à des fins précises, explicites et légitimes et non traitées d'une manière incompatible avec ces fins ; un traitement ultérieur à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ne doit pas être considéré comme incompatible avec les fins initiales.
- c) Adéquat, pertinent et limité à ce qui est nécessaire en ce qui concerne les fins pour lesquelles ils sont traités.
- d) Précis et, le cas échéant, tenu à jour ; toutes les mesures raisonnables doivent être prises pour s'assurer que les données personnelles inexactes, compte tenu des fins pour lesquelles elles sont traitées, sont effacées ou corrigées sans délai.
- e) Conservé sous une forme qui permet d'identifier les sujets de données pour une durée non plus longue que nécessaire aux fins pour lesquelles les données personnelles sont traitées; les données personnelles peuvent être stockées pendant de plus longues périodes dans la mesure où les données personnelles seront traitées uniquement à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques sous réserve de la mise en œuvre des mesures techniques et organisationnelles appropriées exigées par le GDPR pour sauvegarder les droits et libertés des individus; Et
- f) Traité d'une manière qui assure une sécurité appropriée des données personnelles, y compris la protection contre le traitement non autorisé ou illégal et la perte accidentelle, la destruction ou les dommages, en utilisant les mesures techniques ou organisationnelles appropriées. »

2. Dispositions générales

- a) Cette politique s'applique à toutes les données personnelles traitées par le Groupe Media Contact.

GRUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

- b) La personne responsable est responsable du respect continu de cette politique par Contact médias de groupe.
- c) Cette politique doit être revue au moins une fois par année.
- d) Le Contact Médias groupe doit s'inscrire auprès de tout bureau/commissaire/organisme statutaire pour se conformer aux lois pertinentes en tant qu'organisation qui traite les données personnelles si un fournisseur de services l'exige.

3. Traitement légal, équitable et transparent

- a) Pour s'assurer que son traitement des données est légal, équitable et transparent, le Contact Médias du Groupe doit tenir un Registre des Systèmes.
- b) Le Registre des systèmes doit être examiné au moins une fois par année.
- c) Les particuliers ont le droit d'accéder à leurs données et toute demande de ce genre faite au Contact Médias du Groupe doit être traitée rapidement.

4. Fins légales

- a) Toutes les données traitées par le Groupe Media Contact doivent être effectuées sur l'une des bases légales suivantes : consentement, contrat, obligation légale, intérêts vitaux, tâche publique ou intérêts légitimes.
- b) Le Contact Médias Groupe doit noter le fondement légal approprié dans le Registre des Systèmes.
- c) Lorsque le consentement est invoqué comme base légale pour le traitement des données, la preuve du consentement d'opt-in doit être conservée avec les données personnelles.
- d) Lorsque des communications sont envoyées à des personnes en fonction de leur consentement, la possibilité pour la personne de révoquer son consentement devrait être disponible et des systèmes devraient être mis en place pour s'assurer qu'une telle révocation se reflète exactement dans les systèmes du Contact avec les médias du groupe.
- e) Minimisation des données

GROUPE MEDIA CONTACT SA

 Avenue Dorothée LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

- f) Le Contact Médias groupe doit s'assurer que les données personnelles sont adéquates, pertinentes et limitées à ce qui est nécessaire en ce qui concerne les fins pour lesquelles elles sont traitées.

5. Précision

- a) Le Contact Médias groupe doit prendre des mesures raisonnables pour s'assurer que les données personnelles sont exactes.
- b) Si nécessaire pour la base légale sur laquelle les données sont traitées, des mesures doivent être mises en place pour s'assurer que les données personnelles sont mises à jour.

6. Archivage / Déménagement

- a) Pour s'assurer que les données personnelles ne sont conservées que nécessaire, le Contact Médias du Groupe doit mettre en place une politique d'archivage pour chaque domaine dans lequel les données personnelles sont traitées et examiner ce processus chaque année.
- b) La politique d'archivage doit tenir compte des données qui devraient/doivent être conservées, pendant combien de temps et pourquoi.

7. Sécurité

- c) Le Contact Médias Groupe doit s'assurer que les données personnelles sont stockées en toute sécurité à l'aide de logiciels modernes qui sont tenus à jour.
- d) L'accès aux données personnelles doit être limité au personnel qui a besoin d'accès et une sécurité appropriée devrait être en place pour éviter le partage non autorisé d'informations.
- e) Lorsque les données personnelles sont supprimées, cela doit être fait en toute sécurité de sorte que les données sont irrécupérables.
- f) Des solutions appropriées de secours et de récupération après sinistre doivent être en place.

8. Violation

En cas de violation de la sécurité conduisant à la destruction accidentelle ou illégale, à la perte, à la modification, à la divulgation non autorisée ou à l'accès à des données personnelles, le Contact médias du Groupe évaluera rapidement le risque pour les droits et libertés des personnes et, le cas échéant, signalera cette violation aux autorités compétentes.

GROUPE MEDIA CONTACT SA

 Avenue Dorothée LIMA, rue 11010
Gbegamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 **+229 95 17 00 16**
contact@groupmediacontact.com

 **RCCM N° : RB/COT/13B 10291**
IFU N° : 3201300930112

II. SÉCURITÉ DE L'INFRASTRUCTURE

Historique des révisions	
Dernière mise à jour	Décembre 2020

GROUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbegamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

9. Énoncé de politique générale

Il n'y a pas d'accès non autorisé aux informations physiques ou électroniques sous la garde du Contact Médias du Groupe. La protection est accordée à :

- a) Dossiers papier sensibles
- b) Équipement informatique utilisé pour accéder aux données électroniques.
- c) Équipement informatique utilisé pour accéder au réseau privé du Groupe Media Contact.

Le Contact médias du groupe sensibilisera les communautés d'utilisateurs à cette politique.

10. But

- a) Assurer le respect de la loi et d'autres contrôles obligatoires et des meilleures pratiques définies dans la norme de sécurité ISO27001 et ISO9001.
- b) Assurer la protection continue des informations personnelles et sensibles que détient et utilise le Contact Médias du Groupe, en particulier toute information classée PROTECT, RESTRICTED ou CONFIDENTIAL.
- c) Veiller à ce que toute protection soit appropriée à la sensibilité de l'information et aux risques associés à la perte d'intégrité, de disponibilité ou de confidentialité de ces renseignements, tout en veillant à ce que les normes minimales obligatoires soient respectées.

11. Portée

La politique définit quelles informations papier et électroniques appartenant à Group Media Contact devraient être protégées et offre des conseils sur la mesure dans laquelle la protection peut être obtenue. Cette politique décrit également les rôles des employés et la contribution du personnel à l'utilisation sûre et sécurisée de l'information sous la garde du Groupe Media Contact. Cette politique devrait être appliquée chaque fois qu'un utilisateur accède aux coordonnées des médias du Groupe ou à l'équipement d'information de ses partenaires.

Cette politique s'applique à tous les endroits où les informations sous la garde du Groupe Media Contact ou de l'équipement de procession de l'information sont stockées, y compris les sites distants. Ce document s'applique à tous les comités, départements, partenaires, employés du groupe Contact médias, employés de sous-traitants fournissant des services à

GRUPE MEDIA CONTACT SA

 Avenue Dorothée LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

Group Media Contact, à des tiers contractuels et à des agents du Contact Médias du Groupe qui utilisent Group Media Contact ont fourni des installations et de l'équipement informatiques, ou qui ont accès aux informations clients de Group Media Contact ou qui en ont la garde.

Tous les utilisateurs doivent comprendre et adopter cette politique et sont responsables d'assurer la sécurité des systèmes du Groupe Media Contact et les informations qu'ils utilisent ou manipulent.

Tous les utilisateurs ont un rôle à jouer et une contribution à apporter à l'utilisation sûre et sécurisée de la technologie et de l'information qu'elle contient.

12. Politique

Application de la politique

- a) Évaluer l'impact de la perte de sécurité
- b) Des directives détaillées sur l'évaluation de la gravité de toute perte de sécurité de l'information (confidentialité, intégrité de la disponibilité) sont contenues dans la Politique de classification et d'accès aux données.

Normes de sécurité de contact avec les médias baseline group

Sécurité physique

La sécurité physique doit commencer par le bâtiment lui-même et une évaluation de la vulnérabilité du périmètre doit être effectuée. Le bâtiment doit avoir mis en place des mécanismes de contrôle appropriés pour le type d'information et d'équipement qui y est stocké. Il peut s'agir, sans s'y limiter, des

- Alarmes installées et activées en dehors des heures de travail.
- Serrures de fenêtre et de porte.
- Barres de fenêtre aux niveaux inférieurs de l'étage.
- Les mécanismes de contrôle d'accès installés sur toutes les portes accessibles (lorsque les codes sont utilisés, ils doivent être régulièrement modifiés et connus uniquement des personnes autorisées à accéder à la zone ou au bâtiment).

GRUPE MEDIA CONTACT SA



Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

- Caméras de vidéosurveillance.
- Zone de réception avec personnel.
- Protection contre les dommages - p. ex., incendie, inondation, vandalisme. Une attention particulière sera accordée aux centres de données et aux salles d'équipement de télécommunications.

Zones sécurisées de base

Tout bâtiment ou chambre au sein du Groupe Media Contact qui ne sont normalement pas ouverts au public est considéré comme un espace sécurisé de base comme un minimum. Tous les bâtiments et salles du Contact médias du Groupe sont considérés comme des zones sécurisées de base à des moments où ils ne sont pas ouverts au public. Dans les zones sécurisées de base, ce qui suit est applicable :

- Les employés doivent afficher leur photo d'identité et mettre au défi toute personne qui n'affiche pas les laissez-passer d'identité de contact avec les médias de groupe appropriés (PhotoID)
- Chaque ministère doit s'assurer que les portes et les fenêtres sont bien sécurisées.
- Les outils/laissez-passer d'identification et d'accès (p. ex., insignes, clés, codes d'entrée, etc.) ne doivent être détenus que par des agents autorisés à accéder à ces zones et ne doivent être prêtés/fournis à personne d'autre.

Zones sécurisées améliorées

La désignation d'une zone sécurisée améliorée tient compte des niveaux d'impact de toutes les données stockées ou traitées dans cette zone ainsi que d'autres risques, y compris le vol, la perte ou les blessures corporelles subies par des personnes dans cette région. Lorsqu'une zone sécurisée améliorée est désignée, tous les visiteurs sont tenus de se connecter et de sortir avec les heures d'arrivée et de départ et sont tenus de porter un badge d'identification.

Lorsqu'une zone sécurisée améliorée contient des éléments clés de l'infrastructure TIC, un membre de l'équipe de gestion de l'information du Groupe Media Contact doit surveiller tous les visiteurs. Des procédures détaillées pour la protection des zones contenant des composants clés de l'infrastructure TIC sont décrites dans le manuel de procédure du Groupe Media Contact pour tous les employés des TIC. Les clés de toutes les zones sécurisées améliorées abritant les principales composantes de l'infrastructure des TIC seront détenues en toute sécurité par la gestion de l'information.

GROUPE MEDIA CONTACT SA



Avenue Dorothée LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

Les clés en double peuvent être détenues en toute sécurité par le service personnel de sécurité du Groupe Media Contact, le cas échéant pour l'inspection de sécurité et en cas d'incendie ou d'urgence. Les clés ne doivent pas être stockées près de ces zones sécurisées.

Répondre aux failles de sécurité pour toute zone sécurisée

Lorsqu'il est nécessaire de communiquer avec les services d'urgence avec le personnel de sécurité local, cela précède habituellement toute autre action. Tout employé peut contacter les services d'urgence ou le personnel de sécurité sur place sans avoir besoin d'une autorisation supplémentaire. Les employés ne doivent pas se mettre eux-mêmes, leurs collègues ou leurs clients en danger de préjudice physique ou de blessure. Signaler les failles de sécurité pour toute zone sécurisée

La déclaration d'une atteinte à la sécurité sert à plusieurs fins, notamment l'enregistrement, l'analyse et la détermination d'une intervention subséquente et la mise en œuvre de mesures préventives. Les employés de Group Media Contact qui n'ont pas d'autorisation d'accès, de vol ou de perte ou toute autre menace à la sécurité dans une zone sécurisée (zone sécurisée de base ou zone sécurisée améliorée) doivent être signalés au gestionnaire de la ligne qui doit, à son tour, en informer le responsable de la sécurité. En plus des exigences de cette politique, les installations locales seront maintenues conformément au document (mise à jour périodique). Tout accès, vol ou perte non autorisé ou toute autre menace à la sécurité dans une zone sécurisée sera signalé à la direction locale qui devra, à son tour, conseiller le directeur de l'établissement pour les locaux en question.

Menaces sur les actifs de l'information

Lorsqu'une atteinte à la sécurité comporte une menace pour la sécurité de l'information, l'incident doit également être enregistré au bureau du Service. L'incident sera ensuite progressé selon la politique et la procédure de gestion des incidents de sécurité de l'information.

Sécurité de l'information sur papier

Les renseignements sur papier (ou non électroniques similaires) doivent être attribués à un propriétaire et à une classification, tel qu'indiqué dans la politique de classification et d'accès des données. Lorsqu'un document est classé et marqué comme PROTECT ou RESTREINT ou CONFIDENTIEL, des contrôles de sécurité de l'information pour le protéger doivent être mis en place. La nature exacte des contrôles sera déterminée par :

- Une évaluation des risques qui tenir compte de la probabilité d'une menace, de la

GRUPE MEDIA CONTACT SA



Avenue Dorothée LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

nature et de la sensibilité du document

- Tout contrôle obligatoire spécifié par la loi, par les exigences de conformité sectorielle ou par les obligations contractuelles

Les mesures appropriées pour protéger les documents peuvent comprendre :

- Classeurs qui sont verrouillés avec les clés stockées loin de l'armoire.
- Coffres-fort verrouillés.
- Stocké dans une zone sécurisée protégée par des contrôles d'accès, en plus de ces contrôles, il stipule que les informations marquées PROTECT, RESTRICTED ou CONFIDENTIAL ne doivent pas être laissées sans surveillance sur un bureau.

Sécurité des équipements TIC

Tous les équipements informatiques généraux doivent être situés dans des endroits physiques appropriés qui :

- Limitez les risques liés aux dangers environnementaux , par exemple la chaleur, le feu, la fumée, l'eau, la poussière et les vibrations.
- Limitez le risque de vol – p. ex., si nécessaire, les articles comme les ordinateurs portables doivent être fixés physiquement au bureau.
- Permettre aux postes de travail traitant des données sensibles d'être positionnés pour éliminer le risque que les données soient vues par des personnes non autorisées. Les PC de bureau ne doivent pas avoir de données stockées sur le disque dur local. Les données doivent être stockées sur les serveurs de fichiers réseau, le cas échéant. Cela garantit que les informations perdues, volées ou endommagées via un accès non autorisé peuvent être restaurées avec l'intégrité maintenue.
- Les serveurs ne résideront pas à l'extérieur des centres de données désignés, qui seront à leur tour considérés comme des « zones sécurisées améliorées » et protégés en conséquence.
- Tous les articles d'équipement doivent être consignés dans un inventaire. Des procédures doivent exister pour s'assurer que l'inventaire est maintenu et à jour.
- Tous les équipements TIC doivent être marqués de sécurité et avoir un numéro d'actif unique qui croise les références à l'inventaire

GROUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbegamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

- Pour les appareils informatiques portables, veuillez vous référer aux stratégies suivantes :
 - Travail à distance et mobile – Politique d'utilisation acceptable
 - Médias amovibles – Politique d'utilisation acceptable

Sécurité de câblage

Les câbles qui transportent des données ou qui supportent les principaux services d'information doivent être protégés contre l'interception ou les dommages. Les câbles électriques doivent être séparés des câbles réseau pour éviter les interférences. Les câbles réseau devraient être protégés par conduit et, dans la mesure du possible, éviter les itinéraires à travers les espaces publics.

Informations sur l'entretien de l'équipement

La gestion de l'information (GI) doit s'assurer que tous les équipements TIC sont maintenus selon les instructions du fabricant et avec toutes les procédures internes documentées pour s'assurer qu'il reste en bon état de fonctionnement. Ce processus :

- Les manuels d'instructions du fabricant doivent être conservés
- La maintenance suit les instructions du fabricant
- Tous les intervalles de service recommandés seront enregistrés et respectés
- Il y aura un processus d'appel pour obtenir de l'entretien et du soutien en cas de panne d'équipement
- Seuls les employés ou les agents compétents et autorisés de la gestion de l'information (GI) entretiendront l'équipement.
- Les historiques de service (registres des travaux de réparation) seront maintenus.
- Toutes les exigences en matière d'assurance seront identifiées
- Les registres des défauts et des mesures correctives seront conservés. Les antécédents de service serviront à appuyer les décisions d'affaires relatives au remplacement en temps opportun de l'équipement vieillissant

GROUPE MEDIA CONTACT SA



Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

Sécurité de l'équipement hors site

L'utilisation de l'équipement hors site doit être effectuée conformément aux politiques suivantes :

- Travail à distance et mobile – politique d'utilisation acceptable
- Médias amovibles – politique d'utilisation acceptable

Les utilisateurs doivent également être conscients de leurs responsabilités en matière de protection des données et être au courant de la Loi sur la protection des données et d'autres lois pertinentes.

Élimination ou réutilisation sécurisée de l'équipement

- Lorsqu'un ordinateur ou un appareil multimédia doit être réutilisé à l'extérieur de l'équipe à laquelle il a été initialement affecté, toutes les données de l'équipement doivent être effacées en toute sécurité avant d'être réaffectées.
- Lorsqu'un ordinateur ou un appareil multimédia a atteint la fin de sa durée de vie utile, toutes les données sur l'équipement seront effacées en toute sécurité, puis éliminées d'une manière respectueuse de l'environnement.
- Lorsqu'il s'agit d'un dispositif multimédia amovible, la politique des médias amovibles doit également être mentionnée.
- Lorsque l'équipement doit être transmis à une autre organisation (p. ex., retourné en vertu d'un contrat de location), le retrait de la date de sécurisation sera effectué avant le transfert d'équipement. Les pratiques d'effacement sécurisé des données feront l'objet d'une vérification périodique par une tierce partie indépendante.

Livraison et réception de l'équipement dans le contact avec les médias du Groupe

- Les livraisons de TIC doivent être signées par une personne autorisée à l'aide d'un processus formel vérifiable. Ce processus doit confirmer que les articles livrés correspondent entièrement à la liste sur la note de livraison.
- Les actifs réels reçus doivent être comptabilisés
- Les zones de chargement et les installations de détention devraient être adéquatement protégées contre l'accès non autorisé et tout accès doit être vérifié.
- L'enlèvement subséquent de l'équipement devrait se faire au moyen d'un processus

GROUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

13. Audit régulier

Les dispositions en matière de sécurité de l'information feront l'objet d'une vérification régulière afin de fournir une évaluation indépendante et de recommander des améliorations à la sécurité au besoin.

Troisième partie : Application de la loi, gouvernance, définitions et références

14. Application des politiques

L'interprétation et l'application de cette politique concernant toute prétendue non-conformité seront entreprises comme suit :

Non-conformité	Groupe d'application de la loi
Employés	Hr
Entrepreneur	Gestionnaire des relations et RH
Visitors/Invité	Guest Relevant Department et RH
Gestion Snier	Hr

Les infractions à cette politique seront soumises à la politique et procédures disciplinaires de Contact Avec les médias de groupe, aux modalités contractuelles et au droit civil et pénal qui sont appropriés.

15. Gouvernance des politiques

Le tableau suivant indique qui, au sein de Group Media Contact, est responsable, responsable, informé ou consulté en ce qui concerne cette politique. Les définitions suivantes s'appliquent :

GRUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbgamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

Fonctions	Description	parties prenantes
Responsable	La personne responsable de l'élaboration et de la mise en œuvre de la politique.	Responsable de la gestion de l'information et responsable de la gestion d'actifs
Responsable	Les personnes qui ont la responsabilité ultime et l'autorité pour la politique.	Agent principal des risques d'information
Consulté	Les personnes ou les groupes à consulter avant la mise en œuvre ou la modification définitive de la politique.	Ressources humaines, Services juridiques
Informé	Les personnes ou les groupes à informer après la mise en œuvre ou la modification de la politique.	Tous les employés de Group Media Contact, les membres de Group Media Contact, le personnel temporaire et les entrepreneurs, les fournisseurs et les organisations partenaires.

16. Examen et révision

Cette politique sera revue comme il est jugé approprié, mais pas moins fréquemment que tous les 12 mois. L'examen des politiques sera entrepris par les chefs de la gestion de l'information et de la gestion des actifs ou leurs délégués.

GRUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

III. POLITIQUE DE SÉCURITÉ DES RÉSEAUX IP

Historique des révisions	
Dernière mise à jour	Décembre 2020

GROUPE MEDIA CONTACT SA

 Avenue Dorothée LIMA, rue 11010
Gbgamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 **+229 95 17 00 16**
contact@groupmediacontact.com

 **RCCM N° : RB/COT/13B 10291**
IFU N° : 3201300930112

17. Énoncé de politique générale

Group Media fournit une large gamme de services au MNO dans toutes les régions africaines, ce qui nécessite une infrastructure informatique sécurisée. Bon nombre des systèmes informatiques qui appuient ces services utilisent le Wide Area Network (WAN) pour transmettre des informations sensibles telles que des transactions critiques, des dossiers de personnel et d'abonnés, ainsi que des données d'entreprise exclusives. Le Groupe Media s'engage à protéger l'intégrité, la confidentialité et la disponibilité de ses systèmes d'information, les informations sensibles que ces systèmes traitent et la confidentialité des informations des abonnés, tout en assurant une gestion efficace et efficiente de ces informations.

18. Définitions

Réseau vaste (WAN)

Pour cette politique, l'WAN est définie pour inclure toutes les lignes et périphériques utilisés pour mettre fin aux services de communication de données d'un fournisseur de services. L'WAN peut également être appelée réseau provincial de données dans diverses ententes avec les fournisseurs de services et autres contrats signés avec des fournisseurs. Les appareils WAN peuvent comprendre des concentrateurs, des routeurs, des commutateurs, des appareils sans fil ou d'autres appareils. Le Comité de sécurité détermine si les appareils sont classés wan ou non. Dans cette définition, les ordinateurs personnels, les serveurs de fichiers, les imprimantes ou d'autres périphériques du Réseau local (LAN) ne sont généralement pas classés dans le cadre de l'WAN. (Voir l'illustration sur la page suivante).

19. Réseau d'entreprise

Pour cette politique, le réseau d'entreprise inclut l'WAN, tel que défini ci-dessus, ainsi que les LAN, y compris les serveurs de fichiers, les ordinateurs personnels, les imprimantes et d'autres appareils informatiques ou de communication de données qui sont utilisés par n'importe quel département, bureau, agence, conseil d'administration ou commission au sein du Groupe Media. Toute autre organisation connectée est considérée comme une entité externe nécessitant une autorisation spécifique pour se connecter et accéder au réseau d'entreprise et est tenue de se conformer à la politique et aux normes de sécurité de l'WAN, y compris toutes les révisions, lorsqu'elle est connectée. Cette définition du réseau

GRUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

d'entreprise a une portée intentionnellement large pour fournir des limites claires au Comité pour les personnes chargées de sa sécurité. (Voir l'illustration sur la page suivante).

D'autres termes utilisés dans le corps de cette politique sont définis dans le glossaire

Le soufflet de figure est une illustration de WAN et de réseau d'entreprise

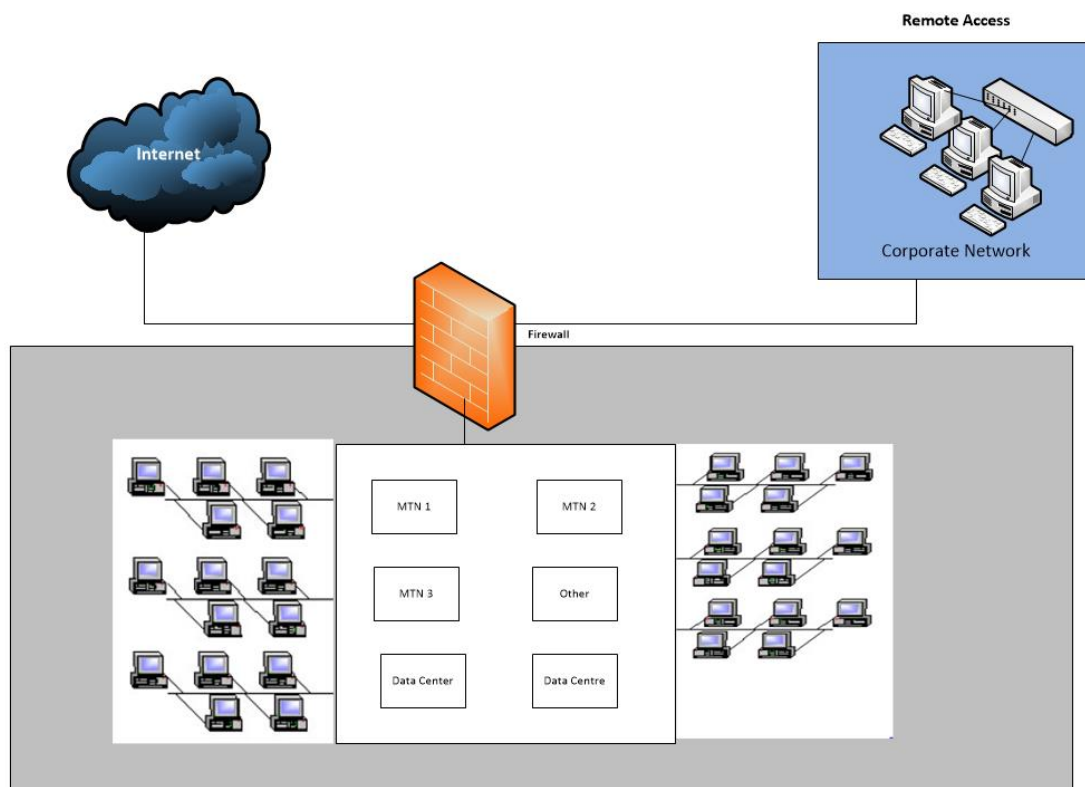


Figure 1: Illustration conceptuelle du réseau WAN, elle n'est pas destinée à être la véritable représentation du réseau réel

20. Objectifs politiques

Les objectifs de cette politique sont les suivants :

- Contribuez à un environnement WAN sécurisé pour tous les ministères, bureaux, agences, conseils d'administration et commissions connectés.
- Fournir un cadre de sécurité uniforme pour assurer l'intégrité, la confidentialité et la disponibilité des systèmes d'information et d'information, au niveau de l'WAN.
- Fournir, en équilibre avec les exigences opérationnelles, les exigences

GROUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

législatives et les accords d'échange d'information, les exigences minimales en matière de sécurité wan.

- Sensibiliser tous les utilisateurs de l'WAN aux besoins en matière de sécurité des technologies de l'information et de l'information en leur fournissant les principes, les exigences et les règles d'utilisation en matière de sécurité.
- Définir les rôles et responsabilités clairs de tous les utilisateurs de l'WAN, en particulier du personnel de sécurité de l'WAN.
- Fournir une base pour élaborer et mettre en œuvre des politiques et des normes supplémentaires qui pourraient être nécessaires pour régler des problèmes de sécurité spécifiques.

21. Application

Cette politique s'applique à tous les MNO connectés au Réseau d'entreprise, bureaux, agences et organisations clientes, ainsi qu'à d'autres utilisateurs authentifiés dans une zone autorisée de l'AJR, comme les organisations commerciales (entités externes). Tout contenu couvert par les politiques ministérielles également visé par ou en conflit avec tout contenu de cette politique est remplacé par cette politique. En outre, cette stratégie remplace toutes les stratégies antérieures liées à la sécurité WAN telles que la stratégie de passerelle pare-feu.

22. Directives politiques

Les directives politiques sont les exigences minimales obligatoires qui doivent être remplies par l'ONM et les entités externes.

Lignes directrices générales sur la sécurité du réseau

- a) L'accès et l'utilisation du réseau de contact avec les médias de groupe doivent toujours être conformes aux politiques et aux normes de sécurité du réseau De contact avec les médias de groupe.
- b) Les mesures de contrôle de sécurité réseau doivent être appliquées de façon uniforme à tous les employés, systèmes informatiques et systèmes de communication
- c) Les renseignements doivent être protégés en fonction de la confidentialité, de la

GROUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

valeur et de la critique; indépendamment des supports sur lesquels il est stocké ou des méthodes par lesquelles il est déplacé.

- d) Les politiques et normes de sécurité du réseau de Contact médias de groupe seront examinées sur une base annuelle, au minimum, afin de s'assurer qu'elles demeurent à jour. L'agent de sécurité et de conformité examinera les procédures de sécurité du réseau et les lignes directrices appropriées sur les fournisseurs sur une base semestrielle, au minimum pour s'assurer que les mesures de sécurité les plus actuelles sont appliquées.
- e) Tous les composants du réseau de contact avec les médias du Groupe devraient faire l'objet d'une vérification annuelle au moins annuelle afin de s'assurer qu'ils restent conformes aux politiques de sécurité du réseau De contact avec les médias du Groupe.
- f) Tous les employés doivent avoir reçu suffisamment de formation et de matériel de référence pour leur permettre de protéger adéquatement le réseau de contact avec les médias du groupe.
- g) L'agent de sécurité et de conformité est chargé d'identifier les écarts par rapport aux politiques de sécurité réseau généralement acceptées et d'entreprendre rapidement des mesures correctives.
- h) Tous les employés actuels de Group Media Contact ainsi que les nouveaux devraient être formés au moins chaque année en ce qui concerne les politiques de sécurité du réseau. La direction de Group Media Contact doit s'assurer que tous les employés lisent, comprennent et signent les politiques de sécurité du réseau Group Media Contact.
- i) La responsabilité et la responsabilité de suivre au quotidien les politiques de sécurité du réseau De contact avec les médias du Groupe sont le devoir de chaque employé.
- j) Les exceptions aux politiques et normes de sécurité réseau ne seront faites que lorsque les coûts de mise en œuvre d'une norme dépassent les avantages en matière de sécurité ou lorsque la mise en œuvre interdira les activités commerciales nécessaires de Contact avec les médias du Groupe.
- k) Les demandes de modification de ces déclarations contenues dans les politiques de sécurité réseau devraient être présentées et approuvées par la direction du Contact Médias du Groupe et le consultant en sécurité des contacts avec les médias du groupe.
- l) les informations clients (c'est-à-dire les factures) doivent être traitées avec le plus

GROUPE MEDIA CONTACT SA

Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

haut niveau de sensibilité et toutes les activités impliquant des informations clients doivent être effectuées conformément aux politiques de sécurité de Group Media Contact de la même manière que les informations internes confidentielles.

Identification/Authentification

- a) Tous les comptes, identités utilisateur et périphériques du Réseau Corporate doivent être identifiables de manière unique.
- b) Les systèmes informatiques du réseau d'entreprise doivent authentifier tous les utilisateurs, applications et périphériques, à l'exception de ceux conçus spécifiquement pour un accès anonyme. Ces exceptions nécessitent l'approbation du Comité de sécurité.

Contrôles d'accès/autorisation

Lan

- a) Permettre à Port Security de protéger le commutateur contre l'épuisement de la table d'adresse MAC.
- b) Permettre à DHCP Snooping de sécuriser les services DHCP d'être usurpés.
- c) Permettre l'inspection dynamique arp pour limiter l'utilisation du protocole de résolution d'adresse (ARP) au trafic valide.
- d) Activez IP Source Guard pour empêcher l'usurpation d'adresse hôte IP.
- e) Permettre à la garde de l'Unité de données du protocole de pont (BPDU) à arbres de protéger la disponibilité du réseau.
- f) Activez IPv6 Router Advertisement Guard pour protéger les appareils contre la communication avec un routeur IPv6 connecté aux ports d'accès aux utilisateurs.
- g) Activez IPv6 DHCP Guard pour protéger les appareils contre la communication avec un serveur IPv6 DHCP connecté aux ports d'accès aux utilisateurs.

Wan

- a) Tous les points d'accès à l'AJJ doivent être approuvés par le Comité de sécurité.
- b) Tous les liens physiques et logiques avec l'AJR destinés à permettre l'accès par des

GROUPE MEDIA CONTACT SA



Avenue Dorothée LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

individus ou des groupes doivent être approuvés par le Comité de sécurité.

- c) Tous les changements et configurations relatifs à l'ADRESSE WAN doivent être approuvés par le Comité de sécurité.
- d) Toute personne, bureau ou réseau connecté au réseau d'entreprise doit exiger que tous les employés acceptent, par le biais d'une entente signée ou électronique, de se conformer aux exigences énoncées dans la politique et les normes de sécurité de l'WAN.
- e) Les demandes d'accès à l'WAN pour une entité externe doivent être faites par l'intermédiaire du représentant de l'Entreprise. Le représentant assume toute la responsabilité de l'entité qui demande l'accès.
- f) Le personnel qui a accès à des informations sensibles ou qui est responsable de fonctions critiques de sécurité informatique telles que les administrateurs réseau et le personnel de soutien technique a besoin d'un contrôle de sécurité.

23. Accès à distance

- a) Tout accès à distance sur des réseaux non sécurisés doit utiliser la technologie approuvée par le Comité de sécurité pour sécuriser, surveiller et filtrer le trafic.
- b) Tous les accès à distance à l'WAN doivent être authentifiés, enregistrés et restreints afin de minimiser le risque pour les actifs wan.
- c) La gestion des services d'infrastructure (ISM) du Bureau d'information en chef doit veiller à ce que l'accès à distance impliquant l'AJJ soit surveillé afin de protéger le profil de sécurité de l'WAN et la confidentialité des renseignements sensibles contre l'accès et la divulgation non autorisés.
- d) Tout appareil qui permet un accès contrôlé par l'utilisateur au réseau d'entreprise, tel qu'un modem sans fil, n'est pas autorisé, sauf lorsque l'autorisation est accordée par le Comité de sécurité.
- e) Tout accès au Réseau corporatif se fait par des voies approuvées.
- f) Tous les utilisateurs qui utilisent les ressources wan à distance doivent accepter, par le biais d'un accord signé ou électronique, de se conformer à ces exigences.

GROUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

24. Pare-feu

- a) Toutes les communications entre le réseau d'entreprise et les réseaux ayant des profils de sécurité différents doivent être protégées par un pare-feu réseau approuvé par le Comité de sécurité.
- b) Tous les pare-feu et leurs configurations doivent être fournis et gérés par le Comité de sécurité, sauf lorsque le Comité de sécurité approuve les organisations clientes pour installer et gérer leurs propres hôtes pare-feu.

25. Fournisseurs de services de télécommunications

- a) Tous les fournisseurs de services qui contractent avec Group Media, tels que les fournisseurs de communications de données ou de services de sécurité, doivent s'engager contractuellement à assurer le maintien du profil de sécurité wan.
- b) Tous les fournisseurs de services qui contractent avec des entreprises de contact avec les médias du Groupe ont accès à la politique et aux normes de sécurité de l'WAN et acceptent de les respecter et de s'assurer qu'elles sont appliquées au sein de leur organisation.
- c) Toute exception à ces directives doit être approuvée par le Comité de sécurité et incluse comme addenda au contrat.

26. Entrepreneurs

- a) Tous les contrats ou accords de service impliquant les installations, la configuration, la gestion ou toute autre application ou serveur résidant sur le réseau doivent inclure des clauses de sécurité appropriées garantissant le respect de la politique et des normes de sécurité de l'WAN.
- b) Toutes les personnes et organisations qui contractent avec Group Media Contact (c.-à-d. consultants, sous-traitants tiers et employés occasionnels et étudiants) ont accès à la politique et aux normes de sécurité de l'WAN et acceptent de s'y conformer.

GRUPE MEDIA CONTACT SA



Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

27. Sécurité physique et environnementale

- a) Un environnement adéquat (p. ex., température, humidité, alimentation de secours) doit être fourni pour assurer un fonctionnement optimal de l'WAN et de l'équipement d'infrastructure commun tel que spécifié dans la documentation de l'WAN.
- b) Des contrôles physiques doivent être mis en œuvre pour empêcher l'accès non autorisé à l'équipement du Réseau d'entreprise, y compris les routeurs, les commutateurs, les supports de câblage et les serveurs d'accès au réseau.
- c) Le Comité de sécurité doit avoir son avis et son approbation finale de toute conception de site où la connectivité WAN est fournie.
- d) L'accès et l'utilisation du réseau de contact avec les médias de groupe doivent toujours être conformes aux politiques et aux normes de sécurité du réseau De contact avec les médias de groupe.
- e) Les mesures de contrôle de sécurité réseau doivent être appliquées de façon uniforme à tous les employés, systèmes informatiques et systèmes de communication
- f) Les renseignements doivent être protégés en fonction de la confidentialité, de la valeur et de la critique ; indépendamment des supports sur lesquels il est stocké ou des méthodes par lesquelles il est déplacé.
- g) Les politiques et normes de sécurité du réseau de Contact médias de groupe seront examinées sur une base annuelle, au minimum, afin de s'assurer qu'elles demeurent à jour. L'agent de sécurité et de conformité examinera les procédures de sécurité du réseau et les lignes directrices appropriées sur les fournisseurs sur une base semestrielle, au minimum pour s'assurer que les mesures de sécurité les plus actuelles sont appliquées.
- h) Tous les composants du réseau de contact avec les médias du Groupe devraient faire l'objet d'une vérification annuelle au moins annuelle afin de s'assurer qu'ils restent conformes aux politiques de sécurité du réseau De contact avec les médias du Groupe.
- i) Tous les employés doivent avoir reçu suffisamment de formation et de matériel de référence pour leur permettre de protéger adéquatement le réseau de contact avec les médias du groupe.

GROUPE MEDIA CONTACT SA



Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

- j) L'agent de sécurité et de conformité est chargé d'identifier les écarts par rapport aux politiques de sécurité réseau généralement acceptées et d'entreprendre rapidement des mesures correctives.
- k) Tous les employés actuels de Group Media Contact ainsi que les nouveaux devraient être formés au moins chaque année en ce qui concerne les politiques de sécurité du réseau. La direction de Group Media Contact doit s'assurer que tous les employés lisent, comprennent et signent les politiques de sécurité du réseau Group Media Contact.
- l) La responsabilité et la responsabilité de suivre au quotidien les politiques de sécurité du réseau De contact avec les médias du Groupe sont le devoir de chaque employé.
- m) Les exceptions aux politiques et normes de sécurité réseau ne seront faites que lorsque les coûts de mise en œuvre d'une norme dépassent les avantages en matière de sécurité ou lorsque la mise en œuvre interdira les activités commerciales nécessaires de Contact avec les médias du Groupe.
- n) Les demandes de modification de ces déclarations contenues dans les politiques de sécurité réseau devraient être présentées et approuvées par la direction du Contact Médias du Groupe et le consultant en sécurité des contacts avec les médias du groupe.
- o) les informations clients (c'est-à-dire les factures) doivent être traitées avec le plus haut niveau de sensibilité et toutes les activités impliquant des informations clients doivent être effectuées conformément aux politiques de sécurité de Group Media Contact de la même manière que les informations internes confidentielles.

28. Synchronisation du temps

Tous les périphériques du réseau d'entreprise doivent se synchroniser avec une source de temps centrale commune.

29. Révocation/résiliation des privilèges wan

Le Comité de sécurité prend les mesures appropriées, y compris la cessation de tout lien ou activité, à tout moment où le Comité de sécurité estime que la sécurité de l'AJJ est ou pourrait être gravement compromise. Lorsque les circonstances le permettent, le Comité de sécurité consulte le titulaire de la demande avant de prendre des mesures. Le Comité de

GROUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

sécurité doit faire un rapport complet sur les mesures prises et les raisons de ces actions.

30. Contrôle du changement

- a) Tous les changements planifiés et planifiés au WAN (power up, power down, modifications de configuration et réinitialisation) doivent être effectués ou autorisés par le Comité de sécurité.
- b) Un processus de contrôle du changement doit être utilisé pour évaluer l'impact sur la sécurité des mises à niveau majeures du système et pour appuyer la recertification et l'accréditation. Le processus de contrôle des changements doit s'assurer que toutes les configurations et modifications du système sont documentées et conservées dans un environnement sécurisé pour des raisons de vérification ou de gestion future des risques.

31. Mécanismes et planification de la gestion des risques de sécurité

- a) La gestion des risques de sécurité fondée sur la diligence raisonnable et les soins exigibles doit être la base principale pour déterminer les garanties de sécurité et le risque résiduel de l'WAN et pour maintenir le profil de sécurité accrédité de l'AJR.
- b) Des réévaluations du profil de sécurité doivent avoir lieu en cas de risque, de système ou d'autres changements technologiques ou organisationnels pertinents.
- c) Avant la mise en œuvre, tous les nouveaux systèmes, ainsi que les ajouts, suppressions ou modifications apportées aux systèmes existants, doivent être examinés afin de s'assurer que le profil de sécurité du réseau d'entreprise n'est pas compromis par le changement.
- d) L'approvisionnement et l'achat de matériel et de logiciels doivent être examinés par l'équipe de gestion de la sécurité du réseau. Le développement et les utilisateurs ayant des privilèges élevés ne doivent utiliser que les logiciels fournis par une personne, un fournisseur ou une organisation connu et digne de confiance.

GROUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

- e) Les réseaux de communication Group Media Contact seront conçus de manière à ce qu'aucun point de défaillance, tel qu'une commutation centrale ou un routeur central, ne puisse perturber le service réseau essentiel à la continuité des activités. Tous les points d'échec qui existent sur les réseaux moins prioritaires doivent être documentés.
- f) Les concepteurs et les développeurs de systèmes doivent toujours suivre les politiques de sécurité réseau pour la conception de systèmes
- g) La sécurité sera un critère de conception fondamental utilisé dans toutes les conceptions de réseaux de données. Bien qu'il soit entendu que d'autres facteurs peuvent et influenceront la conception finale dans la mesure du possible, les considérations de sécurité doivent être prises en considération dans tout exercice de conception.
- h) Chaque conception de système doit avoir des dispositions pour le recouvrement des erreurs et une piste de vérification. Tous les processus assistés par ordinateur doivent impliquer une intervention humaine avant d'entreprendre toute action qui pourrait entraîner une interruption de service ou un temps d'arrêt de service soutenu.
- i) Une seule fonction primaire doit être implémentée par composant système et en cas d'environnement de virtualisation, une fonction doit être implémentée par machine virtuelle.
- j) Tous les nouveaux contrôles de sécurité du système doivent être testés avant la mise en œuvre.
- k) Les logiciels en développement doivent être strictement séparés des logiciels de production. Cette séparation doit se faire par l'intermédiaire de systèmes et de réseaux informatiques physiquement et logiquement séparés dans la mesure du possible.
- l) Les fonctions de test doivent être exécutées séparément des environnements de production et de développement. Les résultats des tests seront entièrement documentés et maintenus en toute sécurité pendant une période raisonnable.
- m) Toutes les modifications apportées aux systèmes de production doivent suivre les politiques de contrôle du changement.
- n) Il n'y aura aucune restriction à l'utilisation de logiciels et d'outils open-source, à condition qu'un examen juridique approprié des licences de code source ait

été accordé, que l'utilisation soit compatible avec cette licence et que le logiciel soit testé de manière appropriée.

- o) Les employés de Group Media Contact ne doivent pas posséder ou utiliser de logiciels ou de matériel de rupture de code qui permettent la copie illégale de logiciels propriétaires, la découverte de mots de passe ou la cryptanalyse de données chiffrées.
- p) La création de tout nouveau réseau doit être vérifiée par l'agent de sécurité et de conformité et approuvée par la haute direction.
- q) L'architecture du réseau doit être clairement documentée.
- r) Toute modification apportée à l'architecture existante doit suivre les politiques et procédures de contrôle des changements, et la documentation pertinente doit être mise à jour immédiatement.
- s) La documentation des systèmes réseau (diagrammes réseau, tableaux de routage, adresses IP) sont des informations très sensibles qui seront réservées aux employés autorisés.
- t) Tous les systèmes qui stockent ou traitent les données sensibles du Groupe Media Contact ou des clients seront protégés à l'aide d'un pare-feu ou d'autres dispositifs de sécurité réseau approuvés, à partir de réseaux externes publics.
- u) Seul le personnel autorisé sera autorisé à accéder à l'équipement du réseau.
- v) Différents niveaux d'accès seront administrés en fonction de la fonction professionnelle, de la responsabilité et de la nécessité de l'accès de l'employé.

32. Certification et accréditation

La certification et l'accréditation de sécurité des systèmes informatiques doivent être effectuées sur le réseau d'entreprise (y compris tout le matériel et les logiciels qui composent le réseau d'entreprise) tout au long du cycle de vie de la planification, de la mise en œuvre et des opérations.

33. Journaux et enregistrements de sécurité

- a) Les journaux appropriés doivent être conservés et examinés selon les prescriptions de la couche d'accès de sécurité LAN
- b) Permettre à Port Security de protéger le commutateur contre l'épuisement de la table d'adresse MAC.
- c) Permettre à DHCP Snooping de sécuriser les services DHCP d'être usurpés.
- d) Permettre l'inspection dynamique arp pour limiter l'utilisation du protocole de résolution d'adresse (ARP) au trafic valide.
- e) Activez IP Source Guard pour empêcher l'usurpation d'adresse hôte IP.
- f) Permettre à la garde de l'Unité de données du protocole de pont (BPDU) à arbres de protéger la disponibilité du réseau.
- g) Activez IPv6 Router Advertisement Guard pour protéger les appareils contre la communication avec un routeur IPv6 connecté aux ports d'accès aux utilisateurs.
- h) Activez IPv6 DHCP Guard pour protéger les appareils contre la communication avec un serveur IPv6 DHCP connecté aux ports d'accès aux utilisateurs.
- i) Tous les incidents de sécurité réels ou présumés doivent être enregistrés et signalés au Comité de sécurité.

34. Rapports et enquêtes sur les incidents

- a) Tous les incidents de sécurité du Réseau d'entreprise doivent être signalés et examinés immédiatement par le propriétaire de l'infrastructure ou de l'application, l'agent de sécurité du client ou désigné, le Comité de sécurité ou d'autres personnes, le cas échéant. Le Comité de sécurité avise les autres agents de sécurité des clients qui pourraient être touchés.
- b) Le Comité de sécurité peut également mener une enquête secondaire auto-instituée, comme l'a demandé le propriétaire de l'infrastructure ou de l'application, l'agent de sécurité des clients ou désigner pour déterminer s'il y a d'autres problèmes de sécurité et les solutions appropriées.

35. Informations/Documentation de sécurité

- a) L'infrastructure wan doit être documentée comme l'exige le Comité de sécurité de temps à autre. Le Comité de sécurité aura accès à cette documentation sur demande pour appuyer les problèmes de sécurité liés à la conception de l'WAN, les opérations de récupération après sinistre, les processus de contrôle des changements, les enquêtes diagnostiques ou informatiques, les inspections visuelles et les audits de sécurité de l'infrastructure WAN.
- b) Les informations et documents de sécurité wan, y compris la configuration, les sauvegardes et les informations diagnostiques, doivent être protégés par mot de passe, stockés physiquement sous clé et publiés uniquement sur approbation du Comité de sécurité. S'ils sont situés sur un site d'entrepreneur, les détails et obligations de protection doivent être abordés dans le contrat.
- c) Les informations de sécurité et les documents à jeter, et qui contiennent des informations sensibles telles que les mots de passe et les adresses IP, doivent être irrémédiablement détruits en toute sécurité par déchiquetage, suppression électronique permanente, ou par d'autres moyens approuvés par le Comité de sécurité.

36. Surveillance/surveillance et protection de la vie privée

- a) Le Comité de sécurité doit surveiller l'A WAN à des fins de performance et de sécurité.
- b) Les initiatives de surveillance conçues pour l'AJJ s'inscrivent dans le cadre des exigences législatives en matière de protection de la vie privée.
- c) L'accès ou le suivi des segments LAN doit être en coopération avec les administrateurs réseau.
- d) Aucune personne ne doit utiliser des renifleurs ou d'autres dispositifs de surveillance sur le réseau d'entreprise à l'insu préalable du Comité de sécurité.
- e) La surveillance du réseau d'entreprise ne doit pas impliquer la lecture du contenu des données à moins qu'elle ne soit requise dans l'exécution des tâches.

GROUPE MEDIA CONTACT SA



Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

- f) Lorsqu'il y a des raisons de croire qu'une personne se livre à des activités inappropriées sur le Réseau corporatif, le contenu des fichiers individuels peut être lu. Cela ne se produirait que dans le cadre d'une enquête approuvée par les autorités compétentes.
- g) Toute enquête sur le contenu des données doit être menée à la suite des droits de la personne applicables et de toute législation provinciale et étato-américaine applicable.

37. Formation à la sécurité

- a) Le Comité de sécurité doit offrir une formation à tout le personnel, aux agents de sécurité des clients ou aux personnes désignées, et à d'autres personnes, au besoin, sur la politique et les normes de sécurité de l'AJJ, y compris l'interprétation et l'application.
- b) Les organisations clientes sont responsables de la formation sur la sécurité de l'WAN au sein de leur organisation et de toutes les entités externes parrainées par elles, tenues d'assurer l'exécution des responsabilités en matière de sécurité décrites dans la politique et les normes de sécurité de l'WAN.

38. Responsabilités

Directeurs généraux (GM)

GM de chaque organisation cliente est responsable de la sécurité globale de tous les renseignements qui lui sont propres.

Directeur de l'information

Le chef de l'information est en outre responsable de l'élaboration stratégique et de l'analyse des politiques, des normes et des processus de sécurité de l'information.

Coordonnateur des politiques de sécurité

Le coordonnateur des politiques de sécurité est chargé d'élaborer, de surveiller et de proposer des révisions de la politique et des normes de sécurité de l'AJJ en coopération avec les parties prenantes de l'AJJ.

Comité de sécurité

Le Comité de sécurité est responsable de la gestion opérationnelle de la sécurité de l'WAN et

GROUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

dirige la mise en œuvre de la politique et des normes de sécurité de l'AJJ en coopération avec l'ISM, les agents de sécurité des clients ou les personnes désignées. Le Comité de sécurité évalue et répond à toutes les demandes liées à l'accès, aux services et à la sécurité de l'WAN.

Sécurité des clients

Un agent de sécurité client ou désigné est la personne assignée au sein de chaque organisation cliente pour exécuter les exigences de sécurité et les communications de son organisation cliente et pour travailler en coopération avec le Comité de sécurité afin d'assurer le respect de la politique et des normes de sécurité de l'WAN.

Organisation cliente

Une organisation cliente est un département, un bureau, une agence ou une entreprise du Groupe Media connecté au Réseau d'Entreprise et est tenue de se conformer à la politique et aux normes de sécurité de l'WAN.

Entité externe

Une entité externe est une organisation ayant des relations d'affaires avec Group Media, parrainée par une organisation cliente et autorisée par le Comité de sécurité, liée à l'WAN. L'entité externe accepte de se conformer à la politique et aux normes de sécurité de l'AJJ.

Gestionnaires et personnel délégué

Les gestionnaires et le personnel délégué, en plus des responsabilités spécifiques citées ci-dessus, doivent avoir d'autres responsabilités spécifiques pour des aspects spécifiques tels que la disponibilité, la mise à niveau et la maintenance du réseau, la surveillance de la sécurité et la déclaration des incidents.

Organisations hébergeant des installations wan

Les organisations hébergeant des installations wan telles que des routeurs, des pare-feu, des placards de câblage et d'autres composants connexes doivent s'assurer que la protection physique des actifs de l'WAN répond à la politique et aux normes de sécurité de l'WAN.

39. Surveillance (de la politique de sécurité de l'AJJ)

Directeur général

Le directeur général de chaque organisation cliente est responsable de la conformité globale à la politique et aux normes de sécurité de l'WAN.

GROUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbegamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

Coordonnateur des politiques de sécurité

Le coordonnateur des politiques de sécurité doit surveiller la mise en œuvre de la politique de sécurité de l'AJM. Cette responsabilité comprend l'évaluation de l'adéquation et de l'efficacité de la politique et des normes. Le coordonnateur des politiques de sécurité coordonne toutes les mesures correctives nécessaires pour régler les problèmes signalés par le Comité de sécurité dans le rapport annuel sur la sécurité de l'AJM. Le coordonnateur des politiques de sécurité doit également veiller à ce que la politique et les normes soient officiellement revues au moins tous les deux ans.

Comité de sécurité

Le Comité de sécurité est chargé de surveiller la sécurité opérationnelle de l'AJJ afin de s'assurer que le profil de sécurité établi est maintenu et que les environnements changeants, les menaces potentielles et l'évolution de la technologie sont pris en compte. Le Comité de sécurité doit faire rapport chaque année au coordonnateur des politiques de sécurité sur l'environnement de sécurité de l'AJM, les problèmes identifiés et les incidents de sécurité, ainsi que l'efficacité de la politique de sécurité de l'AJM.

Gestion des services d'infrastructure (ISM)

L'ISM doit surveiller le respect de la politique et des normes de sécurité de l'WAN pour tous les systèmes informatiques de leur juridiction. L'ISM avise le Comité de sécurité et le coordonnateur des politiques de sécurité de demander un examen des politiques.

Agent de sécurité des clients ou désigné

L'agent de sécurité du client ou désigné doit surveiller la conformité à la politique et aux normes de sécurité de l'WAN pour tous les systèmes informatiques de sa compétence. L'agent de sécurité du client ou désigné doit aviser le Comité de sécurité et le coordonnateur des politiques de sécurité de demander un examen des politiques.

40. Enquêtes

Toutes les demandes, demandes ou commentaires doivent être transmis à

CIO : Directeur de l'information

41. Glossaire

Contrôle d'accès

Un ensemble de procédures effectuées par le matériel, les logiciels et les administrateurs

GROUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

pour surveiller l'accès, identifier les utilisateurs qui demandent l'accès, enregistrer les tentatives d'accès et accorder ou refuser l'accès.

Accréditation

Approbation par le gestionnaire responsable de l'exploitation d'un système de technologie de l'information à l'aide d'un ensemble particulier de mesures de protection.

Authentification

Le processus de détermination de la question de savoir si une personne, un poste de travail, un système ou une procédure est admissible à accéder à des renseignements précis ou à effectuer certaines opérations. La validation par mot de passe, par exemple, est une forme d'authentification. L'authentification peut également être une mesure destinée à valider une transmission ou un message et le Comité de l'initiateur.

Hôte bastion

Un serveur qui est durci contre les attaques et peut donc être utilisé comme un composant essentiel de la sécurité réseau. Les pare-feu et les routeurs de criblage sont des exemples d'hôtes bastion.

Certification

Un examen par le personnel qualifié des mesures de sécurité mises en œuvre par un système de technologie de l'information contre les exigences de sécurité du système.

Organisation cliente

Voir Accountabilities.

Confidentialité

La sensibilité des renseignements ou des biens à la divulgation non autorisée, enregistrée comme hautement confidentielle, confidentielle ou protégée, chacune d'entre elles implique un certain degré de dommage en cas de divulgation non autorisée.

Entrepreneur

Un tiers impliqué dans la gestion directe de l'WAN ou de n'importe quelle partie de celui-ci, très souvent en vertu d'un accord de gestion ou de communication de données de l'WAN. Les entrepreneurs sont tenus de se conformer à la politique et aux normes de sécurité de l'WAN.

Réseau d'entreprise

Voir Définitions Définitions

Soins dus

Une attention ou une prudence raisonnable que l'on peut attendre d'une personne moyenne dans les circonstances.

GROUPE MEDIA CONTACT SA



Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

Diligence raisonnable

Une mesure de prudence à laquelle on peut s'attendre d'une personne raisonnable et prudente qui est responsable de certains aspects de la gestion des risques pour la sécurité. Il porte avec lui un niveau de responsabilité plus élevé que la « diligence raisonnable ».

Entité externe

Voir Accountabilities. Responsabilités

Pare-feu

Un dispositif de sécurité réseau positionné entre des réseaux avec différents profils de sécurité qui garantissent que toutes les communications qui tentent de se déplacer entre les réseaux sont conformes au profil de sécurité configuré

Intégrité

La qualité ou l'état d'être précis ou complet.

Modem (Modular-Demodulator)

Un appareil qui convertit les signaux numériques utilisés par les ordinateurs et les signaux analogiques utilisés par le téléphone ou le système de télécommunication connexe qui permet aux ordinateurs de communiquer à distance. Dans la politique et les normes de sécurité wan, un modem comprend tout appareil de télécommunications tel qu'un modem commuté, modem câble, modem ligne dédiée, appareil sans fil ou ligne d'abonné numérique (DSL) dispositif.

Moniteur

L'activité visant à s'assurer que l'information et les biens, ou les garanties qui les protègent, sont vérifiés par le personnel de sécurité ou les moyens électroniques avec suffisamment de régularité pour satisfaire à la politique et aux normes de l'AJJ.

Profil de sécurité

Un niveau de sécurité minimum acceptable pour l'AJM établi par la mise en œuvre de la politique et des normes de sécurité de l'AJM.

Comité de sécurité

Voir Accountabilities. Toutes les références au Comité de sécurité dans ce document désignent de temps à autre le Comité de sécurité ou un délégué nommé par le DPI.

Incident de sécurité

Un événement ou une situation qui entraîne un compromis d'informations sensibles, d'actifs, de fonctionnalités ou une perte de disponibilité ou d'intégrité.

Gestion des risques de sécurité

Le processus par lequel les ressources sont planifiées, organisées, dirigées et contrôlées pour s'assurer que le risque d'exploitation d'un système informatique demeure dans des limites

GROUPE MEDIA CONTACT SA



Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

acceptables à un coût optimal.

Fournisseur

Un tiers impliqué dans la gestion directe de l'WAN ou de n'importe quelle partie de celui-ci, très souvent dans le cadre d'un contrat de gestion ou de communication de données wan. Les exceptions à la politique et aux normes de sécurité de l'WAN, le cas échéant, sont documentées dans l'accord de service.

Synchronisation du temps

Processus visant à s'assurer que tous les appareils de l'WAN ont le même temps pour assurer l'exactitude des enregistrements et des journaux.

Menace

Tout événement ou acte potentiel qui pourrait causer un ou plusieurs des éléments suivants : divulgation non autorisée, destruction, enlèvement, modification ou interruption d'informations sensibles, d'actifs, de services ou de blessures aux personnes. Une menace peut être délibérée ou accidentelle.

Évaluation des menaces et des risques

Une évaluation, basée sur l'efficacité des garanties de sécurité existantes ou proposées, des risques d'exploitation des vulnérabilités.

Réseau nontrusted

Un réseau, comme Internet, qui n'a aucune base pour qu'un utilisateur ait confiance et assurance dans sa sécurité inhérente.

GROUPE MEDIA CONTACT SA



Avenue Dorothée LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

IV- POLITIQUE LOGICIELLE ET D'APPLICATION

Historique des révisions		
Dernière mise à jour	2020	Braise

GROUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbgamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 **+229 95 17 00 16**
contact@groupmediacontact.com

 **RCCM N° : RB/COT/13B 10291**
IFU N° : 3201300930112

42. Énoncé de politique générale

Group Media Contact assurera l'utilisation acceptable de logiciels et d'applications par les employés, les entrepreneurs et les tiers.

43. But

Le but de ce document est d'énoncer la politique logicielle et d'application de Group Media Contact et de ses filiales et associés. Toutes les politiques gmc existantes s'appliquent à la conduite des employés et des parties prenantes en ce qui concerne les logiciels, en particulier (mais sans s'y limiter) les éléments suivants :

- Politique de courriel
- Politique des tiers
- Politique du réseau IP
- Politique de protection des données
- Politique de classification des données
- Politique d'utilisation acceptable d'Internet.
- Stratégie de mot de passe.

44. Portée

Ce document s'applique à tous les employés, ministères, partenaires, employés du GMC, tiers contractuels et agents du GMC qui ont accès aux systèmes d'information ou à l'utilisation de l'information à des fins de contacts avec les médias du groupe.

45. Définition

Cette politique doit toujours être appliquée sur le matériel informatique, les logiciels, les applications ou les systèmes d'information du GMC.

46. Risques

Group Media Contact reconnaît qu'il existe des risques associés à l'accès et au traitement de l'information par les utilisateurs pour mener des activités officielles de GMC.

GROUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

Cette politique vise à atténuer les risques suivants :

- Achat de logiciels
- Utilisation et développement de l'application
- Utilisation et installation de logiciels

Le non-respect de cette politique pourrait avoir un effet significatif sur le fonctionnement efficace de la GMC et entraîner des pertes financières et une incapacité à fournir les services nécessaires à nos clients.

47. Acquisition de logiciels

Tous les logiciels acquis par GMC doivent être achetés dans le cadre du processus normal d'approvisionnement par le Service des achats. Les logiciels ne peuvent pas être achetés au moyen de cartes de crédit d'entreprise, de petites caisses, de voyages ou de budgets de divertissement.

Les canaux d'acquisition de logiciels sont limités pour s'assurer que GMC a un enregistrement complet de tous les logiciels qui ont été achetés pour les ordinateurs GMC et peuvent enregistrer, prendre en charge et mettre à niveau ces logiciels en conséquence. Cela inclut les logiciels qui peuvent être téléchargés et/ou achetés sur Internet.

En aucun cas les logiciels personnels ou non sollicités (y compris les économiseurs d'écran, les jeux, les fonds d'écran, etc.) ne devraient être chargés sur une machine GMC car il existe un risque sérieux d'introduction d'un virus.

48. Enregistrement logiciel

Le GMC utilise des logiciels dans tous les aspects de son activité pour soutenir le travail effectué par ses employés. Dans tous les cas, chaque logiciel est tenu d'avoir une licence et le GMC ne tolérera pas l'utilisation d'un logiciel qui n'a pas de licence.

Le logiciel doit être enregistré au nom de GMC et du département dans lequel il sera utilisé. En raison du roulement du personnel, les logiciels ne seront jamais enregistrés au nom de l'utilisateur individuel.

Le système d'information (SI) tient un registre de tous les logiciels GMC et conservera une bibliothèque de licences logicielles. Le registre doit contenir :

- a) Le titre et l'éditeur du logiciel.

GROUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

- b) La date et la source de l'acquisition du logiciel.
- c) L'emplacement de chaque installation ainsi que le numéro de série du matériel sur lequel chaque copie du logiciel est installée.
- d) L'existence et l'emplacement des copies de back-up.
- e) Numéro de série du logiciel.
- f) Détails et durée des arrangements de support pour les mises à niveau logicielles.

Les logiciels sur les réseaux locaux ou plusieurs machines ne doivent être utilisés que conformément au contrat de licence.

Group Media Contact détient des licences pour l'utilisation d'une variété de produits logiciels sur tous les systèmes d'information GMC et le matériel informatique. Ce logiciel appartient à l'éditeur de logiciels et la copie de ces logiciels est une infraction en vertu de la Loi sur le droit d'auteur, les dessins et modèles et les brevets, à moins qu'il ne soit autorisé par le fabricant de logiciels.

Il est de la responsabilité des utilisateurs de s'assurer que tous les logiciels de leur équipement informatique sont sous licence.

49. Applications

Le composant d'application de tous les systèmes d'information, qui est développé en interne ou acheté auprès d'un tiers, est conçu en utilisant des principes d'ingénierie de sécurité. Ces principes d'ingénierie de sécurité sont appliqués à l'ensemble du cycle de vie de l'élément d'application au moyen d'une méthodologie de cycle de vie de développement des systèmes qui inclut des considérations de sécurité à toutes les étapes du cycle de vie.

En outre, l'élaboration de l'élément d'application d'un système d'information comprend la création et l'exécution d'un test de sécurité et d'un plan d'évaluation. Les résultats des tests et de l'évaluation sont documentés et partagés avec les principaux intervenants. L'élément d'application de tous les systèmes d'information sépare logiquement les fonctionnalités de l'utilisateur des fonctionnalités administratives de sorte que l'interface pour l'un ne peut pas être utilisée pour faire fonctionner l'autre.

Procédure de traitement des demandes

Les applications seront développées selon des méthodologies définies qui imposent la sécurité :

- Les processus de développement devraient faire usage de normes et de processus documentés et reproductibles.

GROUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

- Une formation en sécurité devrait être dispensée à l'équipe de développement.
- La gestion de la qualité devrait être effectuée tout au long du processus de développement.
- Le code doit être développé dans un environnement dédié et sécurisé.
- Le code doit être stocké dans des référentiels solidement entretenus.

50. Installation logicielle

Le logiciel ne doit être installé par l'IS, IT Helpdesk qu'une fois que les exigences d'enregistrement ont été remplies. Une fois installé, le média d'origine sera conservé dans une zone de stockage sûre entretenue par l'IT Helpdesk. Les logiciels ne peuvent pas être utilisés à moins d'être approuvés par le chef de département de l'IS ou leur représentant désigné.

Shareware, Freeware et Public Domain Software sont liés par les mêmes politiques et procédures que tous les autres logiciels. Aucun utilisateur ne peut installer de logiciel libre ou d'évaluation sur les systèmes du GMC sans l'approbation préalable des services d'information ou d'un service équivalent.

51. Développement d'applications et de logiciels

Tous les logiciels, systèmes et développement de données pour le GMC ne doivent être utilisés qu'aux fins du GMC.

Le logiciel ne doit pas être modifié ou modifié par un utilisateur à moins qu'il n'y ait un besoin commercial clair. Toutes les modifications apportées au logiciel doivent être autorisées avant la mise en œuvre de la modification. Une procédure complète devrait être en place et devrait inclure, sans s'y limiter, les étapes suivantes :

1. Les demandes de modification affectant un actif logiciel doivent être approuvées par le propriétaire de l'application ou de l'actif logiciel ou par le Conseil consultatif modifié (CAB)
2. Toutes les demandes de modification devraient déterminer si le changement est susceptible d'avoir une incidence sur les arrangements de sécurité existants et celles-ci devraient ensuite être approuvées.
3. Un registre devrait être maintenu des niveaux d'autorisation convenus.
4. Un enregistrement doit également être maintenu de toutes les modifications apportées à l'application/logiciel.
5. Les modifications apportées aux logiciels qui doivent être apportées avant que

GRUPE MEDIA CONTACT SA



Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

l'autorisation puisse être accordée doivent être contrôlées.

52. Matériel informatique personnel

Les ordinateurs Group Media Contact sont des actifs appartenant à GMC et doivent être maintenus à la fois légaux et exempts de virus. Seuls les logiciels acquis dans le cadre des procédures décrites ci-dessus peuvent être utilisés sur les machines GMC.

Les utilisateurs ne sont pas autorisés à apporter des logiciels de la maison (ou toute autre source externe) et de le charger sur les ordinateurs GMC. En général, les logiciels appartenant à GMC ne peuvent pas être rentrés chez eux et chargés sur l'ordinateur d'un utilisateur s'il réside également sur un ordinateur GMC. Si un utilisateur a besoin d'utiliser un logiciel à la maison.

53. Utilisation abusive des logiciels

GMC veillera à ce que les pare-feu personnels soient installés le cas échéant. Les utilisateurs ne doivent pas tenter de désactiver ou de reconfigurer le logiciel Personal Firewall.

Il incombe à tout le personnel de GMC de signaler toute mauvaise utilisation de logiciels connus au chef de département du département IS approprié].

Selon la Loi sur le droit d'auteur, les dessins et modèles et les brevets, la reproduction illégale de logiciels est passible de dommages-intérêts civils et de sanctions pénales. Tout utilisateur de Group Media Contact qui fabrique, acquiert ou utilise des copies non autorisées de logiciels fera l'objet de mesures disciplinaires, le cas échéant, dans les circonstances. GMC ne tolère pas la duplication illégale des logiciels et ne le tolérera pas.

54. Conformité aux politiques

Si un utilisateur est reconnu coupable d'avoir enfreint cette politique, il peut faire l'objet d'une procédure disciplinaire de GMC. Si une infraction criminelle est considérée comme avoir été commise, d'autres mesures peuvent être prises pour aider à poursuivre les contrevenants.

Si vous ne comprenez pas les répercussions de cette politique ou comment elle peut s'appliquer à vous, demandez conseil au chef de la gestion des risques.

GRUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

55. Gouvernance des politiques

Le tableau suivant indique qui, au sein de Group Media, est responsable, informé ou consulté en ce qui concerne cette politique. Les définitions suivantes s'appliquent :

- a) Responsable : la personne responsable de l'élaboration et de la mise en œuvre de la politique.
- b) Responsable : la personne qui a la responsabilité et l'autorité ultimes pour la politique.
- c) Consulté : la personne ou les groupes à consulter avant la mise en œuvre ou la modification finale de la politique.
- d) Informé : la personne ou les groupes à informer après la mise en œuvre ou la modification de la politique.

Responsable	Responsable de la gestion de l'information et responsable du développement et de l'ingénierie
Responsable	Comité directeur des systèmes d'information et agent principal des risques d'information (SIRO)
Consulté	Groupe de direction de l'information (GS), Ressources humaines, Services juridiques
Informé	Tous les employés de Group Media Contact, les membres de Group Media, le personnel temporaire et les entrepreneurs, les fournisseurs et les organisations partenaires

56. Examen et révision

Cette politique sera revue comme il est jugé approprié, mais pas moins fréquemment que tous les 12 mois.

L'examen des politiques sera entrepris par l'IS.

GRUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

57. Messages clés

- Tous les logiciels acquis doivent être achetés par l'intermédiaire de l'IS Procurement un département
- En aucun cas, les logiciels personnels ou non sollicités ne doivent être chargés sur une machine GMC.
- Chaque logiciel est tenu d'avoir une licence et le GMC ne tolérera pas l'utilisation d'un logiciel qui n'a pas de licence.
- Les modifications non autorisées apportées au logiciel ne doivent pas être apportées.
- Les utilisateurs ne sont pas autorisés à apporter des logiciels de la maison (ou toute autre source externe) et de le charger sur les ordinateurs GMC.
- Les utilisateurs ne doivent pas tenter de désactiver ou de reconfigurer le logiciel Personal Firewall.
- La reproduction illégale de logiciels est passible de dommages et intérêts civils et de sanctions pénales.

GROUPE MEDIA CONTACT SA



Avenue Dorothée LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

V- POLITIQUE DE CLASSIFICATION DES DONNÉES ET DE CONTRÔLE DE L'ACCÈS

Historique des révisions	
Dernière mise à jour	Décembre 2020

GROUPE MEDIA CONTACT SA

 Avenue Dorothée LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

Domaines : Classification et contrôle des actifs

Communications et gestion des opérations

Sécurité physique et environnementale

Gestion des incidents de sécurité de l'information

58. Énoncé de politique générale

Responsabilité des services d'information (SI)

On s'attend à ce que tous les employés de l'IS qui rencontrent des informations internes sensibles de Group Media Contact se familiarisent avec cette politique de classification des données et utilisent constamment ces mêmes idées dans leurs activités quotidiennes de contact avec les médias du groupe. Les informations sensibles sont des informations confidentielles ou restreintes, et les deux sont définies plus tard dans ce document. Bien que cette politique fournit des orientations générales, afin d'assurer une protection cohérente de l'information, on s'attend à ce que les employés du SI appliquent et élargissent ces concepts pour répondre aux besoins des activités quotidiennes. Ce document fournit un modèle conceptuel pour l'IS pour classer l'information en fonction de sa sensibilité, et un aperçu des approches requises pour protéger l'information basée sur ces mêmes classifications de sensibilité.

S'attaque aux risques majeurs

Le système de classification des données is, tel que défini dans ce document, est basé sur le concept de la nécessité de savoir. Ce terme signifie que l'information n'est divulguée à aucune personne qui n'a pas un besoin légitime et démontrable d'affaires de recevoir l'information. Ce concept, lorsqu'il est combiné avec les stratégies définies dans ce document, protégera les coordonnées des médias du Groupe contre la divulgation, l'utilisation, la modification et la suppression non autorisées.

59. Informations applicables

Cette politique de classification des données s'applique à toutes les informations électroniques dont IS est le dépositaire.

GROUPE MEDIA CONTACT SA



Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

60. Procédures

Contrôle d'accès

Chacune des exigences politiques énoncées dans le présent document est fondée sur le concept de la nécessité de savoir. Si un employé de l'IS n'est pas clair comment les exigences énoncées dans cette politique devraient être appliquées à toute circonstance, il doit appliquer de façon conservatrice le concept du besoin de savoir. Ces renseignements ne doivent être divulgués qu'aux personnes qui ont un besoin commercial légitime de l'information.

Contrôles d'accès au système

Les contrôles appropriés doivent être mis en place pour authentifier l'identité des utilisateurs et valider l'autorisation de chaque utilisateur avant de permettre à l'utilisateur d'accéder aux informations ou services du système. Les données utilisées pour l'authentification doivent être protégées contre l'accès non autorisé. Des contrôles sont en place pour s'assurer que seuls les membres du personnel ayant l'autorisation appropriée et le besoin de savoir ont accès aux systèmes de contact avec les médias du Groupe et à leurs ressources. L'accès à distance doit être contrôlé par des mécanismes d'identification et d'authentification.

Décisions d'octroi d'accès

L'accès aux informations sensibles aux contacts avec les médias du groupe ne doit être fourni qu'après l'autorisation écrite du propriétaire des données. Les demandes d'accès seront présentées au propriétaire des données à l'aide du modèle de demande d'accès. Les dépositaires des renseignements concernés doivent renvoyer toutes les demandes d'accès aux propriétaires concernés ou à leurs délégués. Les besoins spéciaux pour d'autres privilèges d'accès seront traités sur demande. La liste des personnes ayant accès à des données confidentielles ou restreintes doit être examinée pour obtenir l'exactitude par le propriétaire des données pertinent à la suite d'un calendrier d'examen du système approuvé par le Bureau du directeur technique et du DPI et la gestion des opérations ou la gestion des risques.

61. Classification de l'information

Propriétaires et informations sur la production

Toutes les informations électroniques gérées par IS doivent avoir un propriétaire désigné.

GROUPE MEDIA CONTACT SA



Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

L'information sur la production est une information couramment utilisée pour atteindre les objectifs de l'entreprise. Les propriétaires doivent être au niveau CTO/CIO ou au-dessus. Les propriétaires sont responsables de l'attribution des classifications de sensibilité appropriées telles que définies ci-dessous. Les propriétaires ne possèdent pas légalement les informations qui leur sont confiées. Ils sont plutôt des membres désignés de l'équipe de gestion des contacts avec les médias du Groupe qui agissent à titre d'intendants et qui supervisent la façon dont certains types d'informations sont utilisés et protégés.

Restreint

Cette classification s'applique aux informations commerciales les plus sensibles qui sont destinées à être utilisées strictement au sein de Group Media Contact. Sa divulgation non autorisée pourrait avoir des répercussions graves et négatives sur Group Media Contact, ses clients, ses partenaires commerciaux et ses fournisseurs.

Confidentiel

Cette classification s'applique aux informations commerciales moins sensibles qui sont destinées à être utilisées au sein de Group Media Contact. Sa divulgation non autorisée pourrait avoir des répercussions négatives sur Group Media Contact ou ses clients, fournisseurs, partenaires commerciaux ou employés.

Public

Cette classification s'applique aux renseignements qui ont été approuvés par la direction de Contact avec les médias du Groupe pour être communiqués au public. Il n'y a pas de divulgation non autorisée de ces renseignements et ils peuvent être diffusés sans préjudice potentiel.

Décisions relatives aux propriétaires et à l'accès

Les propriétaires de données doivent prendre des décisions quant à savoir qui sera autorisé à avoir accès à l'information et aux utilisations auxquelles ces renseignements seront mis. Ils doivent prendre des mesures pour s'assurer que les contrôles appropriés sont utilisés dans le stockage, la manipulation, la distribution et l'utilisation régulière de l'information électronique.

62. Réutilisation et élimination des objets

Les supports de stockage contenant des informations sensibles (c'est-à-dire restreintes ou confidentielles) doivent être vides avant de le réaffecter à un autre utilisateur ou de s'en débarrasser lorsqu'ils ne sont plus utilisés. Il ne suffit pas de supprimer les données des médias. Une méthode doit être utilisée qui efface complètement toutes les données. Lors de l'élimination des supports contenant des données qui ne peuvent pas être complètement

GROUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

effacées, elles doivent être détruites d'une manière approuvée par le directeur de la sécurité de l'IS.

63. Sécurité physique

Accès aux centres de données

L'accès au centre de données doit être physiquement restreint de façon raisonnable et appropriée.

Accès aux installations

Tout l'équipement réseau (routeurs, commutateurs, etc.) et les serveurs situés dans le siège social et toutes les installations doivent être sécurisés lorsqu'aucun personnel de Contact médias du Groupe, ou entrepreneurs autorisés, n'est présent. Physiquement sécurisé est défini comme verrouillé dans un endroit qui refuse l'accès au personnel non autorisé.

Considérations spéciales pour l'information restreinte

Si des informations restreintes doivent être stockées sur un ordinateur personnel, un ordinateur portable, un assistant numérique personnel ou tout autre système à utilisateur unique, le système doit se conformer aux garanties de contrôle d'accès aux données approuvées par la haute direction de l'IS et de l'entreprise. Lorsque ces utilisateurs n'accèdent pas ou n'utilisent pas activement les informations restreintes sur une telle machine, ils ne doivent pas quitter la machine sans se déconnecter, invoquer un économiseur d'écran protégé par mot de passe ou restreindre autrement l'accès aux informations restreintes.

Logiciel de cryptage de données

Les employés et les fournisseurs de Group Media Contact ne doivent pas installer de logiciel de cryptage pour chiffrer des fichiers ou des dossiers sans le consentement écrit exprès d'IS Security.

64. Transfert d'informations

Transmission au-dessus des réseaux

Si les données restreintes des contacts avec les médias de groupe doivent être transmises sur n'importe quel réseau de communication externe, elles ne doivent être envoyées que sous forme cryptée. Ces réseaux comprennent les systèmes de messagerie électronique, Internet, etc. Toutes ces transmissions doivent utiliser un réseau public virtuel ou un logiciel

similaire tel qu'approuvé par l'équipe de sécurité de l'information.

Transfert vers un autre ordinateur

Avant que toute information restreinte puisse être transférée d'un ordinateur à un autre, la personne effectuant le transfert doit s'assurer que les contrôles d'accès sur l'ordinateur de destination sont proportionnés aux contrôles d'accès sur l'ordinateur d'origine. Si une sécurité comparable ne peut pas être assurée par les contrôles d'accès du système de destination, les informations ne doivent pas être transférées.

65. Sécurité logicielle

Stockage sécurisé du code objet et source

Le code objet et source du logiciel système doit être stocké en toute sécurité lorsqu'il n'est pas utilisé par le développeur. Les développeurs ne doivent pas avoir accès à modifier les fichiers de programme qui s'exécutent en production. Les modifications apportées par les développeurs doivent être implémentées en production par les opérations techniques. À moins que l'accès ne soit acheminé via une interface d'application, aucun développeur ne doit avoir plus que la lecture de l'accès aux données de production. De plus, toute modification apportée aux applications de production doit suivre le processus de gestion du changement.

Test

Les développeurs doivent au moins effectuer des tests unitaires. Les tests finaux doivent être effectués par l'équipe d'assurance de la qualité ou la population d'utilisateurs cible.

Sauvegardes

Les données sensibles doivent être sauvegardées régulièrement, et les supports de sauvegarde doivent être stockés dans un environnement sécurisé.

66. Gestion des clés

Protection des clés

Les clés publiques et privées doivent être protégées contre les modifications et substitutions non autorisées.

Procédures

Des procédures doivent être en place pour assurer la bonne génération, la manipulation et

l'élimination des clés ainsi que la destruction de matériaux de keying obsolètes.

Sauvegarde des clés

Des procédures sont en place pour protéger tous les documents cryptographiques, y compris les certificats. Is Security doit recevoir des copies des clés pour la sécurité.

GROUPE MEDIA CONTACT SA

 Avenue Dorothée LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 **+229 95 17 00 16**
contact@groupmediacontact.com

 **RCCM N° : RB/COT/13B 10291**
IFU N° : 3201300930112

VI- STRATÉGIE DE MOT DE PASSE

Historique des révisions

Dernière mise à jour	Décembre 2020
----------------------	---------------

GRUPE MEDIA CONTACT SA



Avenue Dorothée LIMA, rue 11010
Gbgamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

67. Aperçu

Cette politique vise à établir des lignes directrices pour créer, maintenir et protéger efficacement les mots de passe lors de Group Media Contact.

68. Portée

Cette politique s'applique à tous les employés, entrepreneurs et affiliés de GMC, et régit l'utilisation acceptable des mots de passe sur tous les systèmes qui se connectent au réseau GMC ou accèdent ou stockent les données GMC.

69. Politique

Création de mot de passe

1. Tous les mots de passe utilisateur et admin doivent être d'au moins [8] caractères de longueur. Les mots de passe et les mots de passe plus longs sont fortement encouragés.
2. Dans la mesure du possible, les dictionnaires de mots de passe doivent être utilisés pour empêcher l'utilisation de mots de passe communs et facilement fissurés.
3. Les mots de passe doivent être complètement uniques et ne pas être utilisés pour tout autre système, application ou compte personnel.
4. Les mots de passe d'installation par défaut doivent être modifiés immédiatement après la fin de l'installation.

Vieillessement du mot de passe

1. Les mots de passe des utilisateurs doivent être modifiés tous les [3] mois. Les mots de passe précédemment utilisés ne peuvent pas être réutilisés.
2. Les mots de passe au niveau du système doivent être modifiés sur une base trimestrielle.

Protection par mot de passe

1. Les mots de passe ne doivent être partagés avec personne (y compris les collègues et les superviseurs) et ne doivent pas être révélés ou envoyés par voie électronique.
2. Les mots de passe ne doivent pas être écrits ou stockés physiquement n'importe où

GROUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 **RCCM N° : RB/COT/13B 10291**
IFU N° : 3201300930112

dans le bureau.

3. Les ID et mots de passe des utilisateurs ne doivent pas être stockés dans un format non chiffré.
4. Les identifiants et mots de passe des utilisateurs ne doivent pas être scénarisés pour activer la connexion automatique.
5. La fonction « Remember Password » sur les sites Web et les applications ne doit pas être utilisée.
6. Tous les appareils mobiles qui se connectent au réseau de l'entreprise doivent être sécurisés avec un mot de passe et/ou une authentification biométrique et doivent être configurés pour verrouiller après 3 minutes d'inactivité.

Application

Il est de la responsabilité de l'utilisateur final d'assurer l'application avec le policy. Si vous pensez que votre mot de passe a pu être compromis, veuillez immédiatement l'incident à GMC et changez le mot de passe.

GROUPE MEDIA CONTACT SA



Avenue Dorothée LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

VII- POLITIQUE DES TIERS

Historique des révisions	
Dernière mise à jour	Décembre 2020

GROUPE MEDIA CONTACT SA

 Avenue Dorothée LIMA, rue 11010
Gbgamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 **+229 95 17 00 16**
contact@groupmediacontact.com

 **RCCM N° : RB/COT/13B 10291**
IFU N° : 3201300930112

70. But

Notre politique de tiers aide le titulaire à utiliser ses ressources informatiques de manière appropriée. La gestion de l'accès à des tiers est essentielle à nos tâches quotidiennes. Nous voulons nous assurer que nos employés comprennent les limites de l'utilisation de leur logiciel tiers d'entreprise. Notre objectif est de protéger les données confidentielles contre les atteintes et de protéger notre réputation, nos biens technologiques et ceux de nos partenaires.

71. Portée

Cette politique s'applique à tous les employés, fournisseurs et partenaires qui se voient attribuer (ou qui ont accès) à un réseau d'entreprise et à un courriel.

72. Accès tiers

Directeur d'école

L'utilisation de tiers doit être formellement gérée et contrôlée afin de s'assurer que tous les risques pour group media contact sont quantifiés, acceptés et minimisés le cas échéant.

Pratiques

Exigences de tiers

- a) Les tiers doivent accepter et signer un contrat juridiquement contraignant et, le cas échéant, un accord de niveau de service (ALS), avant d'avoir accès à l'infrastructure informatique de Group Media Contact.
- b) Les tiers doivent signer une entente de confidentialité standard approuvée
- c) Lorsque l'un d'eux est en vigueur, les tiers doivent accepter de se conformer aux règles du Code de conduite applicables au réseau, au système ou au service consulté. Cela peut généralement inclure l'obligation de ne pas se connecter ailleurs (y compris de retour à l'infrastructure d'entreprise propre à des tiers) sans autorisation préalable.
- d) Les tiers doivent fournir tous les détails de la connectivité à partir des systèmes accédant à l'infrastructure de contact avec les médias du Groupe, en particulier si cela inclut des connexions à d'autres tiers ou réseaux publics. Des preuves de barrières ou de pare-feu appropriés, etc. doivent être fournies.
- e) Les tierce parties doivent coopérer avec Group Media Contact au cours de l'enquête sur tout incident et devraient travailler avec Group Media Contact pour parvenir à une conformité continue aux politiques de sécurité informatique de Group Media Contact.

GROUPE MEDIA CONTACT SA

 Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

- f) Selon la nature du service fourni, Group Media Contact peut demander un droit de vérification pour s'assurer que les contrôles sont suivis et pour enquêter sur tout incident. Des tiers sont priés de coopérer avec Group Media Contact dans l'élaboration d'un tel accord.
- g) Tout le personnel tiers, les entrepreneurs et les sous-traitants qui participent à l'accès au système de contact avec les médias de groupe ou à l'infrastructure réseau doivent être informés de ces exigences et être liés par ces exigences.
- h) Les utilisateurs tiers doivent être identifiables individuellement et responsables de leurs actions, ce qui exclut l'utilisation de comptes partagés ou d'équipe. Si les comptes partagés sont inévitables, le tiers doit s'engager fermement à ce qu'il soit tenu entièrement responsable des actions de son personnel, de ses entrepreneurs ou de ses agents.
- i) Des tiers peuvent être tenus de fournir des éléments de preuve (à un niveau suffisamment élevé) de leurs procédures et contrôles de gestion de la sécurité interne et de leur méthode d'application de la loi pour démontrer leur capacité de satisfaire à ces exigences. Cela peut inclure la sélection du personnel, la formation et les procédures disciplinaires.
- j) Les tiers doivent protéger adéquatement l'accès aux ressources qui accordent l'accès à l'infrastructure de contact avec les médias du groupe, tant au niveau physique que logique. Cela peut nécessiter la localisation de l'équipement dans une zone verrouillée séparément avec des contrôles sur son accès.
- k) Tout accès commuté par des tiers à des systèmes ou réseaux de contact avec les médias de groupe, ou à la propre infrastructure de tiers si l'accès aux ressources de Contact médias de groupe est alors rendu possible, doit être soumis à une « authentification forte ».
- l) L'accès aux systèmes ou réseaux de contact avec les médias de groupe dans l'infrastructure des réseaux publics tels que l'Internet ou les réseaux publics commutés par paquets doit également être fortement authentifié (et ne peut être accordé).
- m) Les tiers doivent détenir en toute sécurité toute information fournie au sujet de Group Media Contact, de ses systèmes, de ses réseaux, de ses applications, de son personnel, de ses procédures et de ses politiques, à moins que ces informations ne soient déjà dans le domaine public. En cas de résiliation du contrat, toutes ces informations doivent être retournées à Group Media Contact et/ou à tous les documents détruits en toute sécurité.
- n) Les informations confidentielles ne doivent pas être envoyées par e-mail non crypté sur des réseaux non fiables tels qu'Internet ou par télécopieur sans contrôle approprié pour s'assurer qu'elles ne sont reçues que par le destinataire prévu.
- o) Lorsque des logiciels, des documents ou d'autres matériaux sensibles sont distribués, des mesures doivent être prises par le tiers pour empêcher l'introduction de virus, de chevaux de Troie ou d'autres modifications non autorisées dans le code.
- p) Les données commerciales ne doivent pas être saisies à des fins diagnostiques ou autres sans l'autorisation préalable de Group Media Contact et des contrôles internes

GROUPE MEDIA CONTACT SA

Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

stricts sur son utilisation. Toutes les données ainsi capturées doivent être détruites en toute sécurité dès que possible. Un journal doit être conservé de toutes ces activités de saisie de données enregistrant l'heure, la durée, le but, l'autorisation et la personne effectuant la saisie des données. Ce journal doit être mis à la disposition de Group Media Contact sur demande et de façon routinière (p. ex., lors des réunions mensuelles d'examen des services). Nb. la suppression simple des fichiers est souvent insuffisante pour supprimer toutes les traces de données. Une méthode sûre d'éradication doit être utilisée.

Exigences internes

- a) Tous les accès des tiers aux ressources, aux données ou aux fonctions d'entreprise informatisées de Group Media Contact sont soumis à un contrat formel ou à un ALS qui traite des questions de sécurité et de contrôle et définit leur responsabilité à leur sujet.
- b) Tous les accès doivent avoir un propriétaire désigné et clair au sein de Group Media Contact qui est responsable et responsable de la relation contractuelle et s'assurer que les activités du tiers sont surveillées par rapport au contrat ou à l'ALS.
- c) Le contrat ou LSL doit être établi et convenu avant la fourniture de l'installation d'accès.
- d) Avant d'accorder un accès à un tiers, une évaluation des risques opérationnels (ORA) devrait être effectuée afin de comprendre les risques et les contrôles atténuants qui peuvent être nécessaires. Cela devrait inclure l'évaluation de tous les systèmes impliquant des données personnelles et leur conformité à la législation sur la protection des données (POPI) où l'accès non autorisé pourrait entraîner des poursuites.
- e) Si l'accès fait partie d'une session informatique collaborative, assurez-vous que le tiers ne peut effectuer que des activités autorisées et afficher les données qu'il est autorisé à voir.
- f) Un inventaire détaillé doit être maintenu pour tous les points d'accès tiers et commutés, ce qui devrait inclure les informations suivantes :
 - Propriétaire du point d'entrée (responsable de l'entretien de cet inventaire)
 - propriétaire (s) de systèmes, d'applications et de données consultés
 - Description et classification des données consultées
 - Raison d'accorder l'accès
 - Autorisation/dispensation d'accès
 - Niveau d'accès autorisé, y compris toute contrainte d'heure de jour ou de fréquence et tous les privilèges spéciaux requis ou refusés aux personnes autorisées à accéder à des cimetières d'authentification
 - Autres contrôles de sécurité utilisés

GROUPE MEDIA CONTACT SA



Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

- Nom d'une tierce partie avec contact(s) pour examen et escalade
 - Détails de l'évaluation des risques effectuée (pointeur à documenter)
 - Date du dernier examen et date du prochain examen.
- g) Des rôles, des responsabilités et des procédures clairs devraient être établis par les deux parties pour :
- date du dernier examen et date du prochain examen
 - liaison en ce qui concerne les questions commerciales
 - liaison sur les questions techniques
 - négociation de contrats
 - négociation et examen des contrats de niveau de service
 - rapports et suivis au niveau du niveau de service
 - l'établissement, la gestion et le soutien technique de la méthode de connexion
 - administration des contrôles de sécurité et des systèmes d'authentification
 - modifier les procédures de gestion
 - rapports d'incidents et escalade
 - l'escalade de toute question liée au service
 - l'escalade de tout problème lié à la sécurité (peut nécessiter des lignes de déclaration distinctes).
- h) Il faudrait envisager d'améliorer les contrôles d'accès au niveau des applications lorsqu'on passera de la prestation de services internes à des services tiers. Il peut être nécessaire de « bien nantis » certains systèmes sensibles ou applications à partir d'un accès tiers possible.
- i) Tous les utilisateurs et en particulier les utilisateurs tiers doivent être limités aux activités autorisées uniquement.
- j) Comme pour les systèmes gérés à l'interne, tous les outils et services publics inutiles de diagnostic du système doivent être supprimés avant de mettre en service un système ou un service, ou des moyens trouvés pour contrôler efficacement leur utilisation.
- k) Lorsque l'accès se fait sur n'importe quel réseau et en particulier sur Internet, limitez les adresses et les protocoles à seulement ce qui est nécessaire. Dans la mesure du possible, restreindre l'accès de tiers aux systèmes autorisés uniquement en installant un tuyau fermé ou en considérablement l'infrastructure de contact avec les médias du Groupe vers les systèmes ou applications cibles.
- l) Les pistes de vérification d'activités importantes menées par des tiers doivent être produites, détenues en toute sécurité pendant une période appropriée et examinées à intervalles réguliers.
- j) Le réseau ou les systèmes accessibles devraient avoir la possibilité de générer une alerte en cas de tentatives d'accès non autorisées ou d'activité non autorisée. Il doit être possible d'arrêter l'accès de manière rapide et contrôlée en cas d'attaque ou d'autre exposition.
- k) Si le tiers est une entreprise avec plusieurs utilisateurs autorisés à accéder aux systèmes de contact avec les médias du groupe, il faut confirmer que tous les

utilisateurs sont informés et comprennent leurs obligations et responsabilités.

- l) Le suivi du respect des exigences du contrat ou de l'ALS doit avoir lieu régulièrement, à des périodes adaptées à la sensibilité des données ou des fonctions consultées. Par exemple, l'accès à des fins de maintenance logicielle doit faire l'objet d'une vérification et d'un examen dès que possible après l'événement.
- m) Group Media Contact doit se réserver le droit de révoquer l'accès du personnel tiers en cas de violation présumée de la sécurité.
- n) Tout accès par des tiers doit être fortement authentifié (lorsque le tiers est considéré comme digne de confiance en tant que membre du personnel) ou soigneusement pare-feu (si une telle authentification et confiance ne sont pas possibles) ou les deux. Tous les pare-feu Internet et Extranet doivent être officiellement approuvés après le processus d'approbation du pare-feu, avant la connexion.
- o) L'accès à des tiers doit être résilié lorsqu'il n'est plus nécessaire. Le processus de résiliation doit inclure la déclaration ou la destruction de tout matériel confidentiel par le tiers et sera la responsabilité du propriétaire de la relation d'affaires au sein de Group Media Contact.

GROUPE MEDIA CONTACT SA

Avenue Dorothée LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112