

POLITIQUE DE SECURITE DES INFORMATIONS

- A) GESTION DES IDENTITES ET DES ACCES
- B) SECURITE DES DONNES
- C) SECURITE DE L'INFRASTRUCTURE
- D) SECURITE LOGICIELLES
- E) SECURITE OPERATIONNELLE
- F) ANNEXE DE SECURITE ET SLA

GROUPE MEDIA CONTACT SA

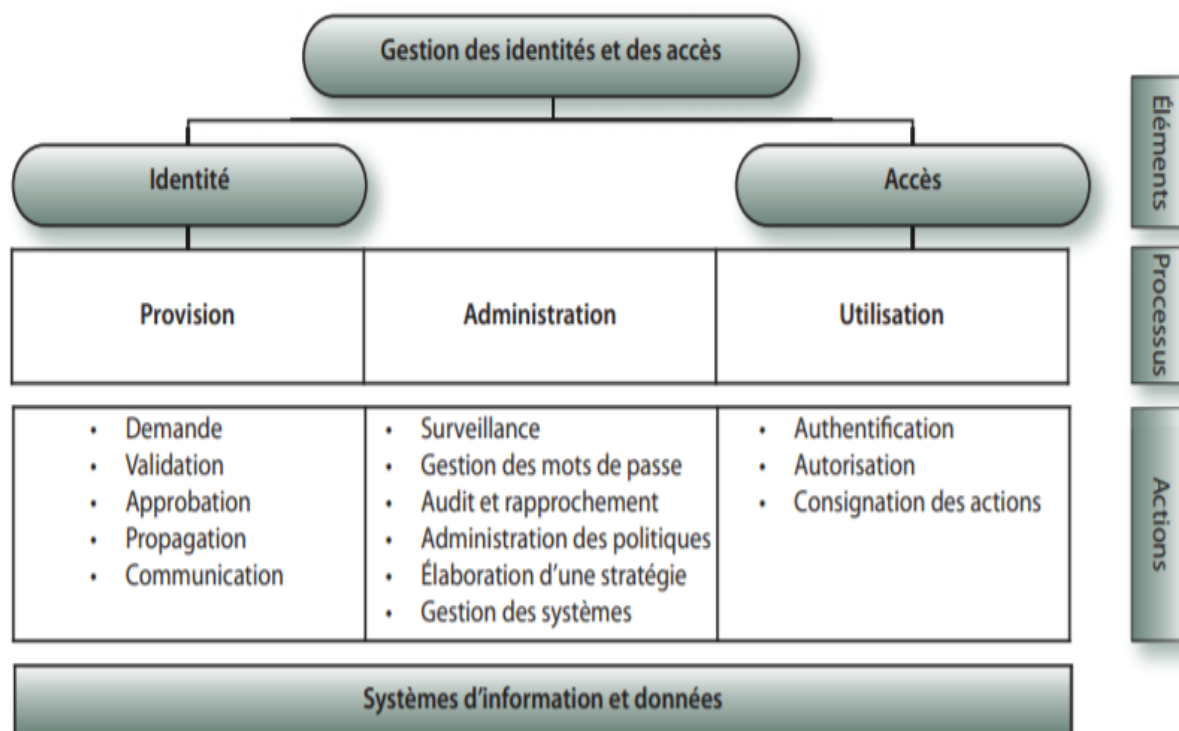
 Avenue Dorothée LIMA, rue 11010
Gbgamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

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

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

A) GESTION DES IDENTITES ET CONTROLE D'ACCES

Afin d'assurer une bonne administration de la sécurité, les systèmes doivent garder trace de toutes les actions significatives et enregistrer l'identité des auteurs de ces événements. L'identité de l'utilisateur détermine ses privilèges et ses droits d'accès à telles ou telles données. En effet, les procédures d'identification et d'authentification des utilisateurs sont nécessaires avant toute stratégie de protection. Il est aussi nécessaire d'appliquer le principe de séparation des privilèges, c'est-à-dire attribuer à chaque utilisateur seulement les privilèges dont il a besoin.



Il existe plusieurs types de droits d'accès :

- Les droits d'accès en consultation (lecture)
- Les droits d'accès en modification (écriture, destruction, création)
- Les droits d'accès en exécution (exécution d'un programme ou d'une commande).

Chaque objet est donc associé à une liste de contrôle d'accès énumérant les utilisateurs

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

autorisés et leurs droits. L'utilisateur souhaitant obtenir des droits d'accès doit avant tout être authentifié, c'est-à-dire que le système de contrôle d'accès doit vérifier que l'identité de l'utilisateur est authentique (par exemple grâce à un mot de passe). L'authentification permet d'assurer la légitimité d'un accès à une ressource. Les utilisateurs ordinaires ont quant à eux des droits d'accès en création, écriture et en destruction à leurs propres données, et des droits d'accès en lecture pour les données partagées. Cependant, pour que cette identité soit correctement administrée et qu'elle ne soit pas usurpée, son authenticité doit être vérifiée. Les utilisateurs accèdent à diverses applications fonctionnant sur des systèmes différents, et doivent souvent saisir leurs paramètres de connexion (identité) à plusieurs reprises. C'est dans ce contexte qu'un service d'authentification unique ou Single Sign-On (SSO) est mis en place. Le SSO est un système d'identification centralisé qui permet d'utiliser un seul et même login pour toutes les applications, et donc à l'utilisateur de ne se loguer qu'une seule fois. L'objectif du SSO est notamment d'avoir un référentiel centralisé des identités et mots de passe auquel les applications s'adressent pour vérifier l'identité d'un utilisateur. Ce principe d'authentification unique a plusieurs avantages pour l'entreprise. Il permet notamment d'offrir un accès simplifié aux applications et donc un certain confort aux employés. Il limite aussi les risques au niveau de la sécurité, car il n'est plus nécessaire de retenir plusieurs mots de passe mais un seul. Aussi, le SSO permet de gérer et de limiter l'accès des utilisateurs au réseau, en une seule fois, c'est-à-dire qu'un utilisateur ne pourra accéder qu'aux applications auxquelles il a un droit d'accès.

MISE EN PLACE DES GPO

Les stratégies de groupes sont des ensembles de paramètres qui s'appliquent aux utilisateurs et ordinateurs. Elles permettent de gérer plus facilement la sécurité d'un poste ou de plusieurs postes dans un Domain. Elles permettent à titre d'exemples de rediriger le dossier Mes Documents, de déployer des Logiciels en fonction des services d'une entreprise ou des utilisateurs. Les GPO existent dès la création d'un Domain, c'est là que sont inscrits les différents fonctionnements du domaine. Il en existe deux types à la création du domaine. Les GPO mis en place dans notre cas nous permettent de contrôler les différents profils et leurs droits. En effet grâce à ces GPO, nous arrivons à restreindre l'accès à certaines ressources

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

des postes de travail en fonction des profils. Par exemple toutes les sessions des téléconseillers n'ont pas le droit d'installer des logiciels tiers sur les postes de travail. Plusieurs GPO ont été mis en place et sont classés en fonction des départements.

FORMATION DES UTILISATEURS

La formation des utilisateurs a pour objectif de les rendre autonome à l'usage des outils et applications qui sont utiles à l'exécution de leurs tâches dans l'entreprise. Elle vise :

- **Informier l'utilisateur :**
 - De la mise en place des journaux d'activités permettant de détecter et de retracer toute activité et tout accès non autorisé ;
 - Qu'en l'absence de moyens sécurisés sur son poste de travail, il doit s'abstenir de transmettre des données sensibles vers ou depuis l'extérieur de l'organisme ;
 - Des sanctions auxquelles il s'expose en cas de non-respect des dispositions réglementaires mises en place en matière de gestion des accès.
- **Sensibiliser l'utilisateur :**
 - À l'importance de choisir un mot de passe sécuritaire, selon les bonnes pratiques en la matière, et de le garder secret en tout temps ;
 - À l'importance de verrouiller son poste de travail lorsqu'il s'absente de son bureau ;
 - Aux contraintes légales et aux moyens de sécurisation de l'information à laquelle il accède ;
 - À l'obligation de signaler, sans délai, toute atteinte à la sécurité de l'information à laquelle il accède.

B) SECURITE DES DONNEES

La mise en place d'une politique de sécurité des données efficace consiste à mettre en œuvre un plan d'action.

- La première étape de notre politique de sécurité des données consiste à évaluer les risques et menaces, leurs conséquences et les vulnérabilités
- Nous avons ensuite défini le périmètre sensible, c'est-à-dire quelles données sont particulièrement essentielles ou confidentielles et nécessitent une protection renforcée :
 - Fichiers utilisateurs,
 - Fichiers serveurs (les points de restaurations),
 - Documents contractuels (employés et clients),
 - Emails,
 - Bases de données de nos applications internes et de production (interactions clients avec le call center),
 - Les enregistrements vocaux, vidéos etc.
- Les matériels utilisés pour protéger les informations déclarées sensibles et confidentielles :
 - L'installation d'un pare-feu (Cisco ASA),
 - Mise en place de VPN pour l'accès à distance ;
 - Contrôle d'accès,
 - Serveur de sauvegarde, etc.
- Enfin, nous communiquons régulièrement avec les services et les salariés de l'entreprise vis-à-vis des règles de sécurité informatique et diffuser aux collaborateurs les procédures (best pratique) et les réactions à adopter en cas de problème. Ces règles concernent l'utilisation des logiciels, de sites internet, le matériel informatique, etc.

Une politique de sauvegarde et restauration des données est mise en place.

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

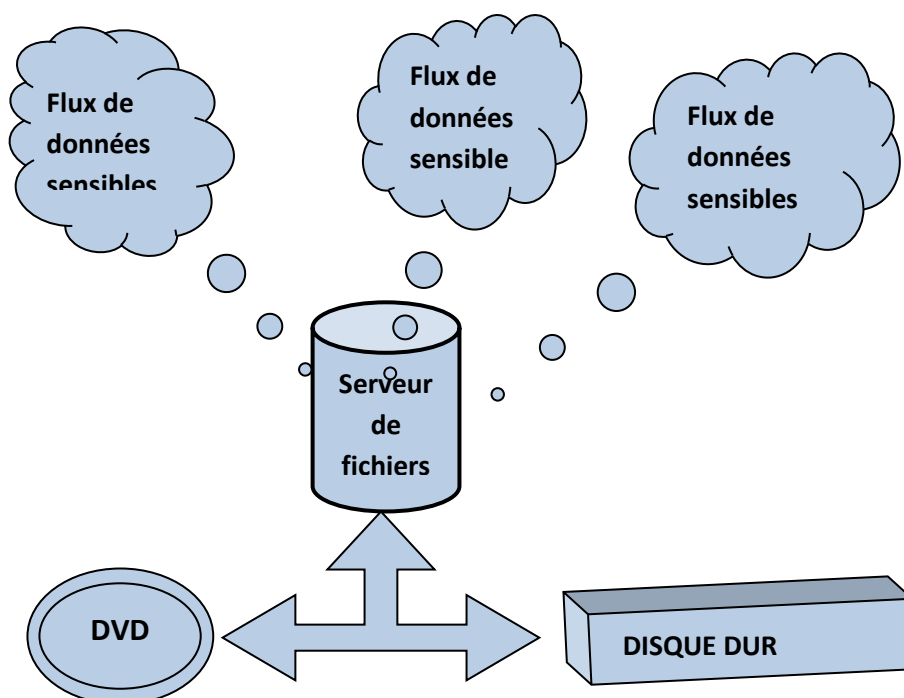
Fréquence/ périodicité de la sauvegarde :

- Des sauvegardes différentielles sont effectuées tous jours à partir de 1h du matin (au moment de baisse du flux d'appels et de la charge du réseau.
- Une sauvegarde complète est effectuée toutes les deux semaines en parallèle à la sauvegarde journalière.

Des sauvegardes spécifiques peuvent être réalisées en parallèle pour des données sensibles comme les données financières de l'entreprise et de production et conservées suivant les obligations légales (s'assurer que les applications ayant généré ces données soient également accessibles et que toutes les données soient bien identifiées, comme par exemple des petits outils de pilotage financier développés en local).

Lieu de stockage des sauvegardes :

Nous avons opté pour une sauvegarde redondante à cause du caractère important des informations que nous traitons. Toutes les sauvegardes sont effectuées sur des serveurs de grande capacité en local et aussi sur le cloud Dropbox (espace où nous avons un espace illimité) pour une longue durée. Les données sur les serveurs en local sont gardées pour une durée d'un (1) an contrairement aux données sur le cloud qui peuvent être conservées sur une très longue période. Ce qui nous permet de les avoir disponibles et accessibles à tout moment (pour respecter le délai de 5 ans demandé).

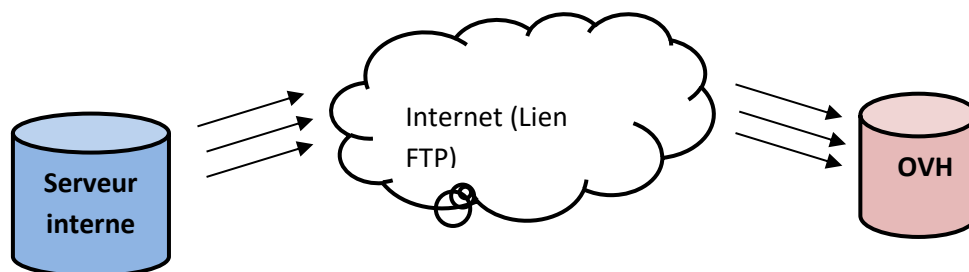


GROUPE MEDIA CONTACT SA

 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



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

C) SECURITE DE L'INFRASTRUCTURE

Sécurité de l'accès aux plateaux de production

Afin d'apporter une sécurité aux personnes et à l'ensemble de l'infrastructure, certaines précautions sont prises :

- Accès contrôlé par les badgeuses (à l'intérieur comme à l'extérieur des portes) ;
- Le bâtiment est surveillé 24h/24 par des agents de sécurité ;
- Les plateaux et tout le bâtiment est contrôlé par des caméras de surveillance 24h/24 et dont les données sont stockées sur un disque de grande capacité
- Mise en place d'un système de détection de fumée/feu
- Mis en place de dispositif d'extincteur de feu
- Des schémas ou circuits d'évacuation du personnel en cas d'incendie affichés partout ainsi que les personnes à contacter
- Bâtiment disposant de deux groupes électrogènes en redondances
- Bâtiment contrôlé par des régulateurs ;

Sécurité d'accès à la salle technique

- Salle bien fermée et contrôlée par un dispositif biométrique ;
- Le fichier de log (badgeuse) est sauvegardé et conservé pour des besoins d'audit ;
- Accès limité seulement aux personnels informatiques ;
- Salle bien aérée par des matériels de climatisation ;
- Salle dotée d'un dispositif de détection de fumée et feu ;
- Salle dotée de plusieurs dispositifs d'extinction de feu ;
- Salle sous surveillance (caméra) ;
- Les serveurs sont alimentés par plusieurs onduleurs ;

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

MEDIA CONTACT BENIN	PROCEDURE CONTROLE PHYSIQUE DES ACCES	
Opération	Etape	Règle
	DEBUT	
Responsable DSI	Définition des zones sécurisées	R1
Gardien	Protéger les zones sécurisées	
Gardien	Consigner la date et l'heure d'arrivée et de départ des visiteurs	
	Limiter l'accès aux zones sécurisées	
Gardien	Identifier les personnes	R2
Gardien	Exiger à tous les visiteurs le port d'un moyen d'identification visible	
Responsable DSI	Contrôle d'identification	
Gardien	Surveiller l'accès des personnes tiers	R3
Responsable DSI	Réexamen et MAJ régulier des droits d'accès aux zones	R4
	FIN	

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

D) SECURITE LOGICIELLES

1. Droits d'accès :

Les identifiants d'ouverture de sessions assurent l'accès aux ressources de base (lecteurs uniquement), et ils ne garantissent pas l'accès aux applications nécessaire à l'exercice des activités. Les droits d'accès permettent de définir, situer et limité les actions utilisateurs sur des fonctionnalités bien définie dans une application. Selon le type des applications, ces droits peuvent varier mais ils comporteront sauf cas exceptionnel un droit d'**administration** de l'application et un droit d'accès aux fonctionnalités principales aux utilisateurs pour qui l'application est destinée. Pour les bases de données, la définition des droits revient au DSI qui les attribue aux administrateurs ou développeur selon leur profil.

2. Autres mesures de sécurité :

D'autres mesures de sécurité sont apportées parmi lesquels, nous pouvons noter :

- **Gestion des évènements de sécurité de l'antivirus :** Les événements de sécurité de l'antivirus sont remontés sur un serveur central pour analyse statistique et gestion des problèmes a posteriori (exemples : serveur constamment infecté, virus détecté et non éradiqué par l'antivirus, etc.). Les mises à jour des bases antivirales et des moteurs d'antivirus sont déployées automatiquement sur les serveurs et les postes de travail par un dispositif prescrit par la DSI.
- **Configuration du navigateur Internet :** Les navigateurs déployés sur le parc informatique n'ont pas d'accès sauf exception par l'équipe informatique locale et des postes de travail nécessitant un accès Internet ou Intranet sont configuré de manière sécurisée (désactivation des services inutiles, nettoyage du magasin de certificats, etc.).
- **Sensibilisation à la lutte contre les codes malveillants :** Les utilisateurs des Systèmes Informatiques de Media Contact sont sensibilisés et responsabilisés à la problématique des codes malveillants. Ils sont informés :
 - Des bonnes pratiques et des règles d'usage à appliquer pour s'en protéger ;
 - Des comportements de vigilance à adopter ;

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



- De la conduite à tenir en cas d'incident de ce type.

- **Mise à jour des Systèmes et Logiciels** : Le maintien dans le temps du niveau de sécurité d'un SI impose une gestion organisée et adaptée des mises à jour de sécurité. Un processus de gestion des correctifs propre à chaque système ou applicatif est défini, et adapté suivant les contraintes et le niveau d'exposition du système. Les correctifs de sécurité des ressources informatiques locales sont déployés en s'appuyant sur les préconisations et outils proposés par les normes de sécurité.

- **Assurer la migration des systèmes obsolètes** : L'ensemble des logiciels utilisés sur le système d'information sont dans une version pour laquelle l'éditeur assure le support, et tenu à jour.

- **Isoler les systèmes obsolètes restants** : Il est nécessaire d'isoler les systèmes obsolètes, gardés volontairement pour assurer un maintien en condition opérationnelle des projets, et pour lesquels une migration n'est pas envisageable. Chaque fois que cela est possible, cette isolation est effectuée au niveau du réseau (filtrage strict), des éléments d'authentification et des applications (pas de ressources partagées avec le reste du Systèmes Informatique).

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

E) SECURITE OPERATIONNELLE

Les mesures mise en place au sein de MEDIA CONTACT afin d'assurer la sécurité du matériel mise a la disposition de l'équipe opérationnelle :

- **Gestion des matériels informatiques fournis à l'utilisateur :** Les postes de travail sont fournis à l'utilisateur, gérés et configurés sous la responsabilité de l'équipe Sécurité Informatique de Media Contact. La connexion d'équipements non maîtrisés, non administrés ou non mis à jour par l'entreprise (qu'il s'agisse d'ordinateur, phones, d'équipements informatiques nomades et fixes ou de supports de stockage amovibles) sur des équipements et des réseaux LAN **est interdite**.
- **Rappel des mesures de protection :** Sensibiliser les télétravailleurs aux risques informatiques (mise ne place des Bonne pratiques)
- **Réaffectation de matériels informatique :** Une procédure de gestion des postes et supports dans le cadre de départs de personnel ou de réaffectations à de nouveaux utilisateurs est mise en place. Elle définit les conditions de recours à un effacement des données.
- **Accès à distance au SI de l'entreprise ou télétravail :** La mobilité et le télétravail multiplient les échanges et les portes d'accès aux données sensibles de l'entreprise. Aujourd'hui plus que jamais, les entreprises ont de plus en plus recours au **télétravail**, imposé actuellement par le **confinement national** lié à la pandémie de Covid-19 ou coronavirus. Or le travail à distance, opéré sur Internet, n'est pas sans risques pour la **protection des données à caractère sensible** de l'entreprise. Nous avons donc revu notre politique de sécurité et l'adapté avec la mobilité de nos managers et téléconseillers car d'une part, on a tendance à être moins vigilant lorsqu'on travaille depuis chez soi, où notre pratique personnelle est moins stricte. Deuxièmement, on est plus exposé à des tentatives d'hameçonnage ou de mails frauduleux. Troisièmement, les réseaux personnels sont moins bien protégés face aux cyberattaques que les réseaux privés d'entreprise. Il est donc indispensable de

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

limiter au maximum les risques en mettant en place les bons outils et en instaurant des pratiques sécurisées.

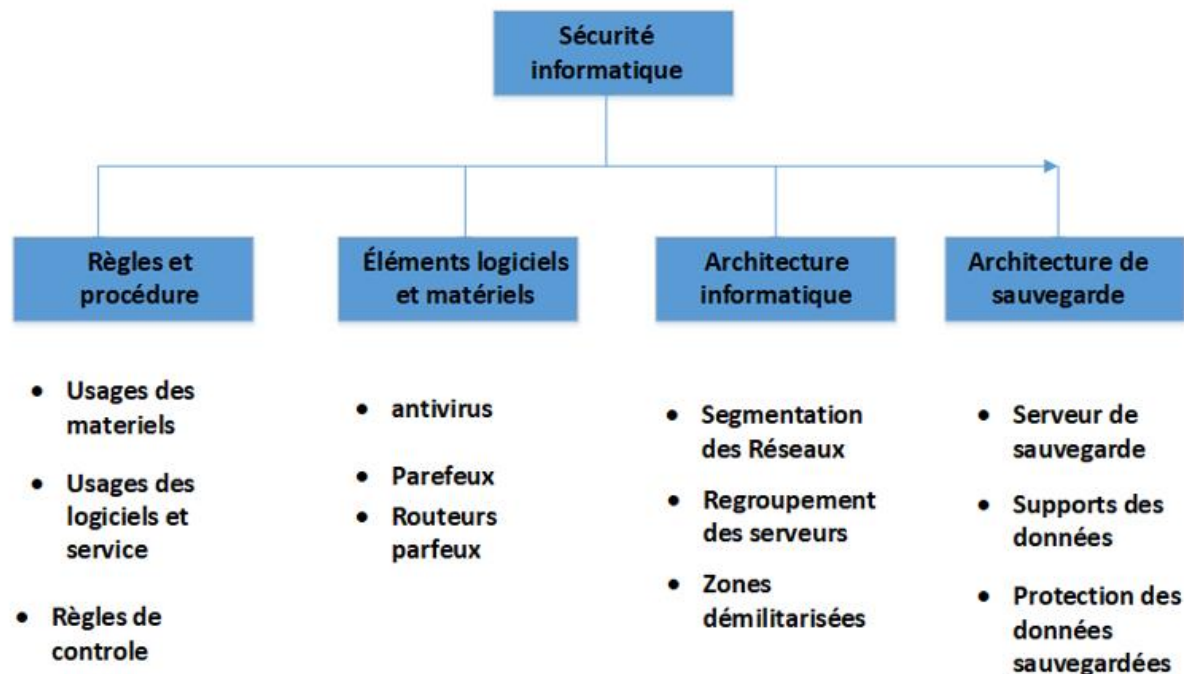
Il existe trois risques majeurs liés au télétravail :

- L'impossibilité pour nos téléconseillers d'avoir accès aux ressources nécessaires pour travailler ;
- La contamination du système de l'entreprise par le biais d'une faille de sécurité de l'ordinateur utilisé par l'employé (et inversement) ;
- La fuite ou la perte de données.

Au regard de cette analyse des risques, voici les actions principales mise en œuvre pour protéger nos données :

- Fournir un ordinateur et un téléphone dédié au travail aux employés.
- Ouvrir un VPN sécurisé pour chaque salarié (Virtual Private Network, réseau informatique virtuel).
- Mettre en place une authentification à deux facteurs pour accéder aux espaces de travail (envoi d'un code par SMS pour se connecter).
- Utilisation des outils de collaboration en ligne (Google Drive et Dropbox pour les fichiers,).
- Restreindre l'accès aux données sensibles au minimum de personnes possible.
- Fournir une liste de contacts directs et fiables à joindre pour chaque question relative à la sécurité.
- Mise en place d'une feuille de route à suivre en cas de cyberattaque (qui contacter, procédures d'urgence, etc.).

F) ANNEXES ET SLA



Les éléments de la sécurité informatique

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

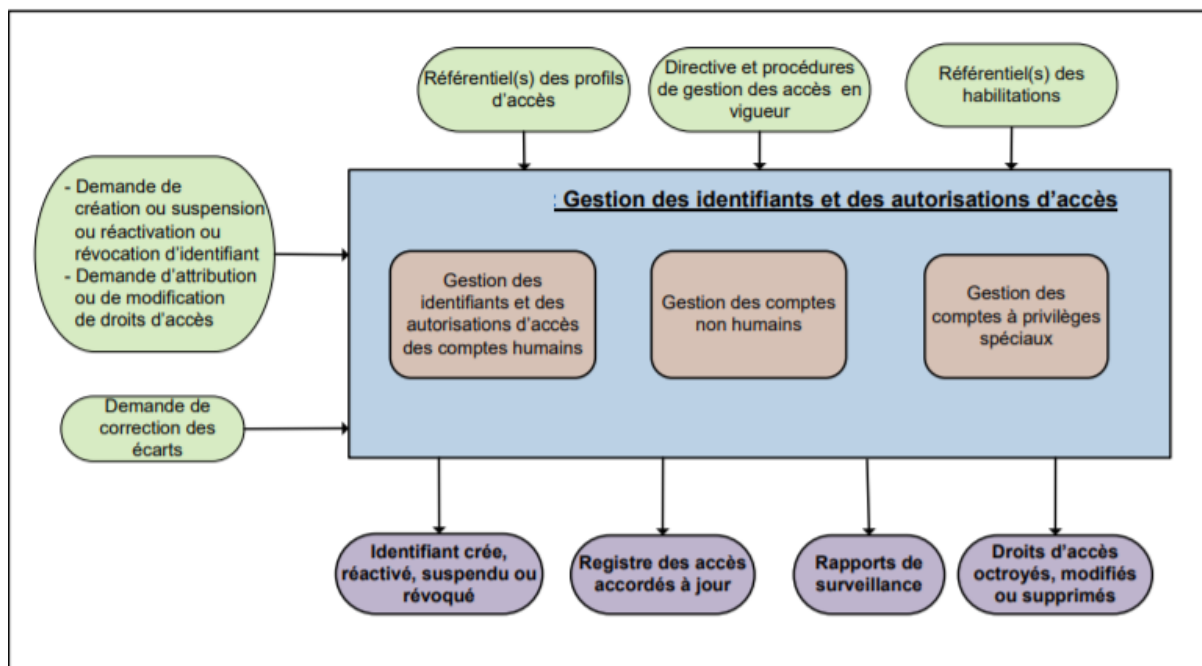


Schéma de gestion des identifiants et des autorisations d'accès

Tels qu'illustré à la figure ci-dessus, l'étape de gestion des identifiants et des autorisations d'accès couvre :

- La gestion des identifiants et des autorisations d'accès des comptes humains, qui consiste à :
- Créer, modifier, enregistrer et résilier les identifiants associés à chaque compte humain, à la demande du gestionnaire ;
- Octroyer, modifier, supprimer les accès autorisés à chaque identifiant, à la demande du gestionnaire ;
- Vérifier si une demande d'octroi d'autorisation d'accès n'engendre pas un conflit de séparation des tâches ;
- S'assurer auprès du gestionnaire qu'une demande d'autorisation d'accès est justifiée lorsqu'elle n'est pas conforme au référentiel des habilitations ;

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

CARTOGRAPHIE DES RISQUES	DETAILS	IMPACT	DEGRE	MESURES/DISPOS ITIONS	SLA (mn)
TECHNIQUES / LOGISTIQUES	Interruption de la fourniture d'énergie	Arrêt de production	Faible	Relai du groupe Electrogène	5
	Panne sur équipement	Arrêt de production	High	Intervention technique	30
	Perte de liaison E1 / Instabilité de la liaison	Coupure d'appels	High	Alerte client	15
	Indisponibilité des applications	Production en mode dégradée (satisfaction des abonnés différée)	Faible	Alerte client	15
	Mauvaise Qualité audio	Grésillement ligne	Medium	****	60
	Crash du serveur (défaillance du serveur)	Perte de données	High	Serveur backup de sauvegarde	60
	Risques environnemental (inondations /incendies,,,,,,,,)	Site inaccessible / Capacité de production réduite	Critical	Mise en place Comité de crise / analyse et plan d'action	180

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