FBC OFFICE SARL

YOUR EXPERT FOR DEVELOPMENT !

POLITIQUE DE CYBERSECURITE

Adoptée en Janvier 2024

TABLE DES MATIERES

INTRODUCTION

Le risque de vol de données, de fraudes et de failles de sécurité peut avoir un impact négatif sur les systèmes, l'infrastructure technologique et la réputation d'une entreprise. Par conséquent, **FBC OFFICE** a élaboré cette politique pour aider à décrire les mesures de sécurité mises en place pour garantir que les informations restent sécurisées et protégées.

L'objectif de cette politique est de protéger les données et l'infrastructure de l'entreprise, de décrire les protocoles et les directives qui régissent les mesures de cybersécurité, de définir les règles d'utilisation professionnelle et personnelle, et de répertorier le processus disciplinaire pour les violations de la politique.

Cette politique s'applique à tous les Experts Associés et non Associés, Partenaires, Employés et Stagiaires et/ou toute personne ayant accès aux systèmes électroniques, informations, logiciels et/ou matériel informatique de FBC Office à l'occasion d'une situation dont l'intervention d'un tiers se trouve indispensable (réparation, maintenance et autres).

I. DONNEES CONFIDENTIELLES

FBC OFFICE définit les "données confidentielles" comme :

- Informations financières non publiées et classifiées ;
- Informations sur les collaborateurs et les partenaires ;
- Clients prospects et données relatives aux prestations ;
- Brevets, processus commerciaux et/ou nouvelles technologies ;
- Mots de passe, affectations et informations personnelles des employés ;
- Contrats d'entreprise et documents juridiques.

II. SECURITE DE L'EQUIPEMENT

Pour assurer la sécurité de tous les appareils ainsi que les informations de l'entreprise, les collaborateurs sont tenus de :

- Garder tous les appareils fournis par l'entreprise, y compris les tablettes, les ordinateurs et les appareils mobiles, protégés par un mot de passe (minimum de 12 caractères) ;

- Sécuriser tous les appareils concernés avant de quitter leur bureau ;

- Obtenir l'autorisation du Gérant avant de retirer les appareils des locaux de l'entreprise ;

- S'abstenir de partager des mots de passe privés avec des collègues, des connaissances personnelles, des cadres et/ou des associés ;

- Mettre régulièrement à jour les appareils avec le dernier logiciel de sécurité.

III. SECURITE DU COURRIER ELECTRONIQUE

La protection des systèmes de messagerie est une priorité élevée, car les e-mails peuvent entraîner des vols de données, des fraudes et transporter des logiciels malveillants tels que des vers et des bogues informatiques. Par conséquent, FBC OFFICE exige que tous les collaborateurs :

- ✓ Vérifient la légitimité de chaque e-mail, y compris l'adresse e-mail et le nom de l'expéditeur ;
- ✓ Évitent d'ouvrir des e-mails et des pièces jointes suspects et de cliquer sur des liens ;
- ✓ Cherchent pour des erreurs grammaticales importantes ;
- ✓ Évitent les titres et les liens de piège à clics ;
- ✓ Contactent le responsable informatique en cas d'e-mails suspects.

IV. TRANSFERT DE DONNEES

FBC OFFICE reconnait les différents risques de sécurité liés au transfert de données confidentielles à l'interne et/ou externe. Pour minimiser les risques de vol de données, tous les collaborateurs doivent :

- S'abstenir de transférer des informations classifiées aux collègues et à des tiers ;
- Ne transférer des données confidentielles que sur les réseaux de FBC Office ;
- Obtenir l'autorisation nécessaire du Gérant ;
- Vérifier le destinataire des informations et s'assurer qu'il a mis en place les mesures de sécurité appropriées ;
- Adhérer à l'accord de confidentialité de FBC Office ;
- Alerter immédiatement le responsable informatique de toute violation, logiciel malveillant et/ou fraudes.

V. MESURES DISCIPLINAIRES

La violation de cette politique peut entraîner des mesures disciplinaires pouvant aller jusqu'au licenciement. Les protocoles disciplinaires de FBC Office sont basés sur la gravité de la violation. Les violations non intentionnelles ne justifient qu'un avertissement verbal, les violations fréquentes de même nature peuvent conduire à un avertissement écrit, et les violations intentionnelles peuvent entraîner une suspension et/ou licenciement, selon les circonstances du cas.

Adoptée à Bobo-Dioulasso au Burkina Faso par l'Assemblée Générale Ordinaire des Associés en sa séance du 15 janvier 2024.