CONTRÔLE D'ACCÈS POLITIQUE

KVKK_P7 VERSION 1.00

KARDELEN PAINT AND CHEMICAL INDUSTRY TRADE LIMITED COMPANY

POLITIQUE DE CONTRÔLE D'ACCÈS

1. Objet et portée

Kardelen Boya met en œuvre des contrôles d'accès physiques et logiques sur les réseaux, les systèmes informatiques et les services utilisés par la Société afin de fournir un accès utilisateur détaillé, auditable et approprié, avec des niveaux d'autorisation adaptés au service fourni, et de garantir et maintenir la confidentialité, l'intégrité et la disponibilité des données conformément à sa politique de sécurité de l'information.

Le contrôle d'accès vise à protéger les intérêts de tous les utilisateurs autorisés des systèmes informatiques utilisés par Kardelen Boya, ainsi que les données fournies par des tiers, en créant un environnement de travail sécurisé, sûr et accessible.

1.1. La présente politique s'applique à toutes les données, informations et systèmes détenus ou exploités par Kardelen Boya, quel que soit le lieu où l'accès aux systèmes informatiques et de communication électronique utilisés par Kardelen Boya est possible. Ses dispositions s'appliquent également à tous les fournisseurs, prestataires, sous-traitants, consultants, bénévoles, personnels accompagnant les études de recherche, étudiants stagiaires et travailleurs temporaires, y compris les tiers et institutions autorisés à accéder aux systèmes informatiques et de communication électronique de Kardelen Boya. Les termes « Utilisateur des ressources informationnelles » ou « Utilisateur », utilisés dans la présente politique, désignent les personnes mentionnées ci-dessus.

1.2. Le site web de la société accessible au public et d'autres informations classées comme « publiquement accessibles ». Les systèmes hors du contrôle de Kardelen Boya ne sont pas couverts par la présente politique. L'accès privilégié aux systèmes, ressources et applications non gérés par l'entreprise relève de la responsabilité du propriétaire du système, de la ressource ou de l'application, et non de Kardelen Boya. Les procédures d'autorisation et de contrôle relatives à l'octroi d'accès à ces ressources sont de la responsabilité de leurs propriétaires.

2. Définitions et rôles des participants

2.1. L'accès aux données, aux informations et aux systèmes n'est autorisé que lorsqu'une nécessité commerciale légitime se présente. L'accès ne peut être accordé que si le propriétaire des ressources informationnelles l'autorise et que toutes les politiques, procédures, principes et conditions applicables sont respectés. Si l'utilisateur n'a plus besoin d'accéder au système, notamment en raison d'un changement de poste, d'un départ à la retraite, d'une cessation d'emploi ou de la finalisation d'un projet, tous les privilèges d'accès définis doivent être révoqués et le droit d'accès à l'information doit être supprimé.

2.2. Les privilèges utilisateur permettent aux utilisateurs d'accéder aux activités spécifiques d'autres utilisateurs. ou elle doit être définie de manière à empêcher la personne concernée d'accéder à des données auxquelles l'utilisateur concerné n'a pas expressément autorisé l'accès, ou d'interférer de quelque manière que ce soit avec celles-ci.

2.3. Les droits d'accès aux entités physiques et logiques seront accordés conformément aux principes du moindre droit d'accès et du besoin d'en connaître.

2.4. Le principe du moindre accès signifie qu'un utilisateur particulier n'a droit qu'aux droits qui lui sont accordés. Cela implique que l'utilisateur ne dispose pas de privilèges d'accès supérieurs à ceux nécessaires à l'exercice de ses fonctions et responsabilités. Pour que le principe des droits d'accès minimaux soit appliqué efficacement, il convient de définir la tâche de l'utilisateur, de déterminer l'ensemble minimal de privilèges d'accès requis pour son exécution, et de limiter les droits d'accès qui lui sont accordés à cet ensemble minimal.

Les autorisations de contrôle d'accès pour tous les systèmes seront soumises à un paramétrage par défaut empêchant les utilisateurs non autorisés d'y accéder, et le principe du moindre privilège sera appliqué, exigeant que tout privilège sur le système d'information qui n'est pas spécifiquement autorisé soit interdit.

2.5. Le principe de sécurité en profondeur consiste à mettre en œuvre une défense de sécurité multicouche afin d'offrir une protection nettement supérieure. Ce principe sera appliqué, exigeant un contrôle d'accès à chaque niveau du système, y compris le réseau, les périphériques matériels, les logiciels système, les applications et les données.

2.6. Séparation des tâches : Si un processus métier implique le traitement d'informations essentielles ou critiques pour l'entreprise, le système doit prévoir une séparation des tâches ou d'autres mécanismes de contrôle compensatoires pour les utilisateurs. Ces mécanismes doivent garantir qu'aucune personne ne détienne l'autorité exclusive sur les actifs informationnels ou les fonctions associées. Par exemple, confier à une même personne la responsabilité d'émettre des chèques et de tenir à jour l'historique des données relatives aux transactions financières constituerait une violation du principe de séparation des tâches.

Dans la mesure du possible, aucune personne ne devrait être seule responsable de la réalisation complète d'une tâche impliquant des informations sensibles, confidentielles ou critiques. De même, aucune personne ne devrait être seule responsable de l'approbation de son propre travail. Lorsque cela est possible, au moins deux personnes devraient coordonner le traitement de l'information pour chaque tâche.

2.7. Utilisation acceptable : Kardelen avant de définir un nom d'utilisateur et un mot de passe. Chaque utilisateur souhaitant être autorisé à se connecter aux systèmes utilisés par Boya doit être informé de la politique d'utilisation acceptable des ressources informatiques et de communication électronique et doit signer la déclaration de sensibilisation à la sécurité de l'information.

2.8. Tous les tiers ayant accès aux données, informations et systèmes de l'entreprise sont tenus de s'abstenir de divulguer toute information que Kardelen Boya considère comme non publique. Pour les tiers employés dans le cadre d'un contrat, d'un bon de commande ou d'un accord de sous-traitance, une clause de confidentialité standard sera intégrée à tous les contrats et bons de commande conclus entre Kardelen Boya et le tiers autorisé à accéder aux données, informations et systèmes de Kardelen Boya. Un accord de confidentialité écrit sera conclu avec toute personne physique ou morale fournissant des services à Kardelen Boya (nécessitant l'accès à des données confidentielles) sans être liée contractuellement à Kardelen Boya.

2.9. Contrôle d'accès : Le contrôle d'accès désigne tout mécanisme permettant d'accéder aux données. Pour accéder aux ordinateurs, l'utilisateur doit d'abord s'authentifier à l'aide d'une méthode appropriée. Le mécanisme de contrôle d'accès compare le nom d'utilisateur attribué à l'utilisateur avec la liste de contrôle d'accès.

Le système contrôle les tâches et opérations que l'utilisateur concerné peut et ne peut pas effectuer.

Les systèmes de contrôle d'accès comprennent les éléments suivants : • Création,
lecture, modification ou suppression de fichiers sur un serveur de fichiers, etc.
permissions de fichiers

• Des programmes tels que le droit d'exécuter un programme spécifique sur un serveur d'applications.
autorisations

• Les droits sur les données, tels que la récupération de données à partir d'une base de données ou la mise à jour d'informations.

Les procédures de contrôle d'accès désignent l'ensemble des méthodes et pratiques utilisées par les propriétaires d'actifs informationnels pour autoriser les utilisateurs à accéder aux données, aux informations ou aux systèmes.

2.10. Authentification : L'authentification désigne le processus de vérification des informations d'identification d'un utilisateur par le propriétaire des ressources informationnelles autorisé à identifier cet utilisateur. Dans les systèmes informatiques, l'authentification s'effectue généralement à l'aide d'un nom d'utilisateur et d'un mot de passe uniques, connus uniquement de l'utilisateur et définis pour celui-ci. Le directeur général peut autoriser d'autres méthodes d'authentification sur recommandation du responsable informatique et du délégué à la protection des données (DPO). 2.11.

Système : Un système désigne un ensemble de ressources informationnelles interconnectées, soumises à un même contrôle réglementaire direct et partageant des fonctionnalités communes. Un système peut comprendre du matériel, des logiciels, des informations, des données, des applications ou une infrastructure de communication. Un système d'entreprise, quant à lui, désigne les systèmes qui traitent l'information pour soutenir les processus métiers en cours. Les systèmes désignés comme systèmes d'entreprise auront des exigences de sécurité définies en fonction des besoins de l'entreprise. 2.12.

Responsabilité individuelle : Chaque utilisateur est individuellement responsable de l'accès aux ressources électroniques fournies et utilisées par Kardelen Boya.
L'accès aux systèmes et réseaux informatiques nécessite l'utilisation d'un identifiant informatique unique attribué individuellement à chaque utilisateur, appelé nom d'utilisateur.
Chaque utilisateur des outils informatiques de Kardelen Boya ne peut accéder qu'aux ressources auxquelles il est autorisé à se connecter. Chaque nom d'utilisateur requiert également l'utilisation d'une clé intelligente, similaire à un mot de passe de connexion, afin d'authentifier l'identité de l'utilisateur lors de l'accès aux données, aux informations ou au système. Les informations relatives aux mots de passe sont considérées comme confidentielles et ne doivent être divulguées à personne. Chaque utilisateur est responsable de la mise en œuvre de mesures de sécurité raisonnables pour empêcher toute utilisation non autorisée de ses informations de mot de passe. Pour plus d'informations, veuillez consulter le Règlement relatif aux procédures et principes concernant la détermination, l'utilisation et la protection des mots de passe des utilisateurs.

2.13. Responsables des actifs informationnels : Les responsables des actifs informationnels déterminent qui peut accéder aux ressources protégées et quels seront les droits d'accès définis (lecture, mise à jour, etc.). Ces droits d'accès seront conformes aux fonctions et responsabilités de l'utilisateur de l'information. Les responsables des actifs informationnels peuvent déléguer certaines de leurs responsabilités administratives à leurs subordonnés, mais ils demeurent responsables des actifs informationnels eux-mêmes. 2.14.

Chefs de service : Les chefs de service jouent un rôle primordial dans la sécurité de l'information chez Kardelen Boya. Ils accèdent au système pour le compte des utilisateurs lorsque cela est nécessaire à l'exécution des processus métier.

Ils sont chargés de documenter les demandes. Les chefs de service sont responsables de la modification et/ou de la révocation des droits d'accès des utilisateurs en cas de changement de leurs responsabilités professionnelles ou de leur statut d'utilisateur de l'information.

3. DIRECTIVES RELATIVES AUX PROCÉDURES DE CONTRÔLE D'ACCÈS

3.1. Kardelen Boya fournira à tous ses employés et fournisseurs tiers les droits d'accès appropriés aux données contrôlées par la Société afin de garantir qu'ils remplissent leurs responsabilités assignées de la manière la plus efficace possible.

3.1.1. Identifiants utilisateur généraux : les identifiants généraux ou de groupe constituent une règle
L'identification et l'utilisation des données de Kardelen Boya ne sont pas autorisées, mais elles peuvent l'être dans des circonstances exceptionnelles si des mécanismes de contrôle adéquats sont en place.

3.1.2. Dans tous les cas, Kardelen Boya sera le fournisseur d'accès Internet.
Afin de respecter ses obligations légales et d'appliquer les dispositions de la Politique d'utilisation appropriée des ressources électroniques, l'identité des utilisateurs disposant d'informations d'identification professionnelle doit être clairement identifiable. L'accès à des informations confidentielles ou sensibles ne peut en aucun cas se faire via un compte utilisateur générique.

3.1.3. Comptes disposant de droits d'accès privilégiés : L'attribution de droits d'accès privilégiés, tels que l'accès administrateur local, administrateur de domaine, superutilisateur et administrateur, sera limitée aux utilisateurs jugés appropriés par la haute direction et ne peut pas être définie par défaut.

3.1.3.1. L'autorisation d'utiliser ces comptes ne sera accordée et documentée explicitement par le directeur général que sur demande écrite d'un cadre supérieur (chef de département, directeur général adjoint).

3.1.3.2. Les équipes techniques prendront des précautions pour éviter d'accorder des droits préférentiels à toutes les équipes afin de prévenir d'éventuelles pertes de confidentialité et/ou d'intégrité.

3.1.3.3. Les comptes privilégiés ne doivent pas être utilisés pour les activités courantes; le Programme
Ces définitions ne peuvent être utilisées que pour l'installation du programme et la reconfiguration du système, et non pour l'utilisation du programme lui-même, sauf si son fonctionnement est autrement impossible.

3.1.4. Le principe du privilège minimum et ce que vous devez savoir : tant sur le plan physique que…
Les droits d'accès aux entités logiques seront accordés conformément aux principes du moindre privilège et en fonction des informations strictement nécessaires.

3.2. Autorisations de contrôle d'accès 3.2.1.

Comptes utilisateurs : Accès aux ressources et services informatiques utilisés par Kardelen Boya
L'accès sera accordé après la saisie du compte utilisateur d'origine et d'un mot de passe complexe.

3.2.2. Les comptes utilisateurs sont créés sous réserve de l'existence d'un dossier employé valide dans le système d'information RH. Pour tout utilisateur sans dossier employé, l'autorisation d'accès est accordée par le chef de service. Par défaut, l'accès est limité à une zone spécifique, un support de stockage et une adresse électronique.

3.2.3. Accès aux informations confidentielles, à accès restreint et nécessaires à l'utilisation au sein d'une unité spécifique uniquement :
Personnes autorisées qui ont besoin d'accéder aux informations pertinentes en raison de leurs responsabilités professionnelles ou commerciales assumées conformément aux lois et accords pertinents avec les parties concernées.

L'accès aux informations concernées sera limité aux employés. Cet accès sera restreint par le biais de pare-feu, de la séparation des réseaux, de procédures d'authentification sécurisées, de listes de contrôle d'accès et d'autres mesures de sécurité jugées appropriées. La responsabilité de la mise en œuvre de ces restrictions d'accès incombe aux responsables d'unité et au service informatique traitant les informations concernées, et sera appliquée conformément aux dispositions de la présente politique. Des méthodes de contrôle d'accès basées sur les rôles seront mises en œuvre afin de sécuriser l'accès à toutes les ressources de fichiers hébergées et gérées par les domaines Active Directory de Kardelen Boya.

3.3. Vérification d'identité et authentification : Tous les ordinateurs connectés au réseau de Kardelen Boya doivent être équipés de mécanismes d'authentification, tels que des identifiants et des mots de passe, afin de permettre le contrôle d'accès. Les systèmes multi-utilisateurs doivent disposer d'identifiants et de mots de passe uniques pour chaque utilisateur, ainsi que de mécanismes permettant de restreindre les droits d'accès. Des outils de contrôle logiciels et matériels, destinés à empêcher tout accès non autorisé à tous les postes de travail, quel que soit leur statut d'accès au réseau, seront mis en œuvre et validés par le responsable informatique.

3.4. Tous les utilisateurs doivent vérifier leur identité avant d'accéder à toute information, donnée ou système. Des procédures de vérification doivent être respectées. À cette fin, un nom d'utilisateur et un mot de passe, définis de manière unique pour chaque utilisateur, seront demandés avant d'accorder l'accès aux réseaux internes de l'entreprise.

3.5. Les utilisateurs doivent s'abstenir d'utiliser les noms d'utilisateur et les mots de passe qu'ils utilisent pour accéder aux ressources système et informatiques utilisées par Kardelen Boya pour accéder à des systèmes extérieurs à Kardelen Boya, y compris les comptes qu'ils utilisent en ligne.

3.6. Sur les systèmes informatiques en réseau, seul l'écran de connexion de l'utilisateur doit afficher les éléments suivants : Le système affichera un message demandant à l'utilisateur de saisir son nom d'utilisateur et son mot de passe pour se connecter. Aucune information relative à l'ordinateur, au système d'exploitation, à la configuration réseau ou à toute autre information spécifique à l'entreprise ne sera communiquée à l'utilisateur avant qu'il ne se soit connecté avec succès à l'aide d'un nom d'utilisateur et d'un mot de passe valides. En cas de saisie incorrecte lors de la connexion, l'utilisateur sera simplement informé de l'échec de la tentative, sans que la cause du problème ne lui soit précisée.

3.7. Identifiants uniques : Chaque identifiant doit être unique et attribué à un seul utilisateur. Si les droits d'accès d'un utilisateur au système sont révoqués, son identifiant ne doit jamais être réutilisé. Chaque identifiant et mot de passe doit être défini pour l'usage exclusif d'une personne. Les identifiants peuvent être partagés par courriel et autres moyens de communication, mais les mots de passe ne doivent jamais être communiqués, quel que soit le moyen utilisé. (L'équipe de support informatique dispose de ses propres droits d'accès et n'a pas besoin d'accéder aux mots de passe des utilisateurs.)

3.8. Procédures d'authentification des utilisateurs : Tous les systèmes d'information de l'entreprise garantissent que seuls les utilisateurs autorisés peuvent utiliser des identifiants avec des mots de passe définis ou des méthodes de chiffrement dynamique plus robustes. Chaque utilisateur est responsable de toutes les actions et transactions effectuées dans les sessions ouvertes à l'aide d'un identifiant et d'un mot de passe ou d'autres mécanismes d'authentification. Les utilisateurs sont tenus de modifier immédiatement leur mot de passe s'ils constatent que leurs informations de connexion ont été divulguées ou utilisées par des tiers. De même, les utilisateurs sont responsables du contrôle d'accès via les informations de session.

Si un utilisateur soupçonne une violation de la confidentialité de ses comptes, il est tenu d'en informer immédiatement le service d'assistance technique du département informatique. Seul le personnel autorisé peut utiliser les identifiants. Il est strictement interdit aux utilisateurs d'autoriser des tiers à effectuer des actions avec leur identifiant. De même, il est interdit aux utilisateurs d'effectuer des actions ou des transactions avec les identifiants d'autres utilisateurs.

3.9. ORDINATEURS PORTABLES ET AUTRES APPAREILS : Les données confidentielles ou sensibles ne peuvent être stockées sur des ordinateurs portables, des iPads, des notebooks, des ordinateurs de poche et autres appareils similaires que si ces derniers sont protégés par les procédures d'authentification décrites ci-dessus. Chaque utilisateur est responsable de la sécurité physique de ces appareils et de la confidentialité des informations et documents qu'ils contiennent.

(point SUPPORTS DE MÉMOIRE PORTABLES : Si des informations non divulguées publiquement par l'entreprise 3.10) sont enregistrées sur des disques souples, des bandes magnétiques, des cartes à puce ou tout autre support de stockage, ces supports doivent être marqués selon le niveau de confidentialité le plus élevé. Lorsqu'ils ne sont pas utilisés, les supports de stockage doivent être conservés dans un endroit sécurisé.

Opérations d'écriture à distance : Des contrôles nécessaires doivent être mis en place pour empêcher l'accès non autorisé aux données confidentielles ou privées (données spécifiées dans la section 3.11) lors des opérations d'écriture à distance. Les utilisateurs doivent s'assurer que les informations confidentielles sont imprimées sur une imprimante sécurisée ou que le processus d'impression est effectué sous la supervision d'une personne autorisée qui peut examiner le document imprimé.

3.12. PARTAGE ET TRANSFERT DE DONNÉES CONFIDENTIELLES ET DE CATÉGORIE SPÉCIALE : Il est interdit aux utilisateurs d'établir des connexions de mémoire électronique, de réseau local, de serveur de transfert de fichiers (FTP), de serveur web ou de modem à des réseaux locaux existants ou à d'autres systèmes multi-utilisateurs dans le but de transmettre des informations sans l'autorisation préalable du service informatique. Seul le personnel expressément autorisé par le responsable informatique et disposant de droits d'accès privilégiés est habilité à mettre en place de tels services.

3.13. ÉLIMINATION ET RECYCLAGE DES ÉQUIPEMENTS ET DES ENVIRONNEMENTS DE STOCKAGE ÉLIMINATION : Si des supports de stockage informatique doivent être envoyés à un fournisseur pour échange, maintenance ou destruction, toutes les données confidentielles et exclusives seront détruites ou dissimulées selon des méthodes approuvées.

SUSPENSION ET ANNULATION DES PRIVILÈGES D'ACCÈS : 3.14.

3.14.1. Accès des utilisateurs aux actifs informationnels détenus par les propriétaires d'actifs informationnels Le responsable des données est chargé d'établir les directives applicables à la révocation des privilèges. Le personnel désigné par ce responsable mettra en œuvre les procédures d'octroi et de révocation des droits d'accès des utilisateurs pour son compte, conformément aux directives établies.

3.14.2. Les chefs de service sont tenus de signaler sans délai tout changement d'affectation ou de statut professionnel des utilisateurs nécessitant une modification de leurs droits d'accès. En cas de cessation d'emploi, le responsable des ressources humaines gère la procédure de révocation des droits d'accès de l'utilisateur concerné à l'ensemble des données, informations et systèmes, et en informe le responsable informatique.

3.14.3. Il incombe aux chefs de service de revoir et de mettre à jour annuellement le système de gestion des droits d'accès des utilisateurs. En cas de modification des droits d'accès, ils procèdent aux ajustements nécessaires dans le système de gestion des comptes utilisateurs.

3.14.4. En cas de cessation de la relation d'un utilisateur avec Kardelen Boya, le responsable du service concerné examinera sans délai les fichiers informatiques et les dossiers papier afin de déterminer la personne chargée de leur conservation et/ou les méthodes appropriées pour leur destruction. Il devra ensuite redéfinir les fonctions de l'utilisateur en déléguant spécifiquement la responsabilité des fichiers précédemment attribués à un nouvel utilisateur désigné. 3.14.5. Les comptes utilisateurs inactifs pendant trois mois seront automatiquement suspendus. Les droits d'accès des utilisateurs reprenant leurs fonctions après un congé, une mission temporaire ou un congé sans solde de plus d'un mois seront redéfinis par le responsable du service concerné.

3.14.6. Session : Si aucune activité n'est détectée sur un poste de travail pendant vingt minutes, le système doit automatiquement assombrir l'écran et mettre fin à la session. La réouverture de session ne doit être autorisée qu'après la saisie d'un mot de passe valide par l'utilisateur. 3.14.7. Gestion des mots de passe : Les mots de passe, les listes de contrôle d'accès et autres informations de contrôle d'accès doivent être chiffrés lors de leur stockage ou de leur transmission sur un réseau. Des mesures de sécurité doivent être mises en place pour empêcher tout accès et toute utilisation non autorisés des mots de passe et des informations de contrôle d'accès stockés. 3.14.8. Les mots de passe ne doivent pas être directement intégrés (codés en dur) dans les logiciels ou les applications afin de permettre leur modification ultérieure.

3.14.9. Les mots de passe attribués aux nouveaux utilisateurs ne doivent être valides que pour leur première connexion. Après s'être connecté, l'utilisateur doit définir un nouveau mot de passe. La même procédure s'applique en cas d'oubli de son mot de passe.

3.14.10. Les mots de passe par défaut des appareils fournis par les fournisseurs doivent être modifiés avant la première utilisation de l'équipement. Cette procédure s'applique aux identifiants des utilisateurs finaux, des administrateurs système et des autres utilisateurs disposant de privilèges.

3.14.11. Les utilisateurs ne doivent communiquer à personne le mot de passe de leur compte utilisateur individuel, y compris à leurs supérieurs hiérarchiques et collègues. Pour le partage de fichiers et d'informations, ils doivent utiliser les répertoires partagés du réseau local, la messagerie électronique, les pages intranet ou les lecteurs de disquettes – des moyens approuvés et autorisés par le service informatique.

3.14.12. Développement du système : Les normes décrites ci-dessous seront utilisées pour empêcher le personnel non autorisé d'accéder aux données générées par l'entreprise et pour améliorer l'intégrité des applications.

Séparation des données d'entreprise, des systèmes de développement et de test : les données générées par les processus métier de l'entreprise doivent être séparées des environnements de développement et de test. Cela garantit une meilleure protection des informations de l'entreprise.

En principe, le personnel travaillant dans les environnements de développement et de test n'est pas autorisé à accéder aux systèmes de l'entreprise. Seuls les chefs de service peuvent autoriser le personnel de développement à accéder aux données de l'entreprise. De même, tous les tests logiciels de l'entreprise doivent traiter des données purgées, en remplaçant les informations et données confidentielles et propriétaires par des données falsifiées. Les systèmes et informations de l'entreprise…

Des processus de contrôle des changements formels et documentés doivent être utilisés pour restreindre et approuver les modifications.
Développement logiciel : Avant le déploiement d'un logiciel en entreprise, les développeurs et autres techniciens doivent éliminer tous les accès privés afin de garantir que l'accès ne soit possible que par des moyens normaux et sécurisés.
Par conséquent, tous les logiciels de porte dérobée et autres raccourcis susceptibles de compromettre la sécurité du système doivent être supprimés. Toutes les procédures de contrôle d'accès, tant au niveau utilisateur qu'administrateur, stipulées dans les politiques et réglementations de sécurité de l'information doivent être définies et activées avant le déploiement des systèmes développés en interne.
Contrôles de migration de l'environnement : Une fois les phases de développement et de test logiciel terminées, une méthodologie appropriée doit être mise en œuvre afin de garantir que la migration du logiciel vers les plateformes d'entreprise se déroule de manière ordonnée et contrôlée. Le personnel de développement d'applications ne doit pas avoir d'accès direct pour téléverser le logiciel dans les environnements informatiques de l'entreprise. Des contrôles nécessaires doivent être mis en place pour empêcher la migration de code applicatif non autorisé vers l'environnement informatique de l'entreprise.
Les privilèges d'accès qui modifient les processus de production de connaissances de l'entreprise doivent être limités aux applications de production de connaissances de l'entreprise. Lors de la définition des privilèges, les utilisateurs du système ne doivent pas être autorisés à modifier les données du système sans restriction. Ils doivent utiliser les données de l'entreprise pour renforcer et protéger l'intégrité des systèmes.
Ils ne devraient pouvoir modifier que les formats précédemment définis.
Les mises à jour des bases de données de l'entreprise doivent être effectuées selon les méthodes désignées et approuvées par la direction. L'utilisation d'outils d'accès direct aux bases de données dans l'environnement de production d'informations de l'entreprise est interdite, car ces programmes peuvent enfreindre les procédures de synchronisation et de réplication des bases de données, les routines de gestion des erreurs de saisie et d'autres mécanismes de contrôle critiques.
Journaux et autres outils de sécurité : Les systèmes informatiques et de communication contenant des données confidentielles ou sensibles doivent consigner tous les événements de sécurité importants. Exemples d'événements de sécurité : modification des identifiants des utilisateurs lors de sessions en ligne, tentatives de devinette de mots de passe, tentatives d'utilisation de privilèges d'accès non autorisés, modifications apportées aux logiciels d'application de l'entreprise, modifications des logiciels système altérant les privilèges des utilisateurs et modifications des sous-systèmes de journalisation.

Le responsable informatique rendra compte régulièrement à la direction des développements, événements, situations, niveaux de conformité aux politiques, changements et autres questions liées à la sécurité d'accès.
Obligations de déclaration : Tout accès non autorisé ou tentative d'accès, vol ou divulgation de mots de passe ou de contrôles d'accès, suspicion de perte, d'altération ou de divulgation de données, et violation des normes, procédures ou politiques de sécurité doivent être immédiatement signalés au superviseur d'unité le plus proche ou à l'équipe de soutien technique informatique en remplissant le formulaire inclus dans le plan de réponse aux violations de données.

4. Contrôle d'accès physique : En raison de la sensibilité des ressources et des données situées dans les installations utilisées par Kardelen Boya, en cas de restrictions d'accès, le contrôle d'accès sera principalement mis en œuvre par Kardelen Boya à l'aide de la technologie RFID.
Ces informations seront fournies via des cartes d'identité. Données de la salle système et de la R&D.
Les systèmes de reconnaissance d'empreintes digitales peuvent également être utilisés pour contrôler l'accès à la zone, sous réserve d'une autorisation écrite préalable du directeur général. Les systèmes de reconnaissance de cartes et d'empreintes digitales ne peuvent être utilisés que pour contrôler l'accès aux zones réservées au personnel autorisé et ne doivent en aucun cas servir à vérifier le respect des horaires de travail.

4.1. En cas de perte de cartes d'identité Kardelen Boya, la situation doit être immédiatement signalée au service informatique.
La personne responsable est avertie. Le responsable informatique veille immédiatement à ce que la carte concernée soit supprimée du système de contrôle d'accès physique de l'entreprise. Une carte de remplacement ne sera délivrée qu'après l'annulation de la carte perdue. Cette nouvelle carte disposera des mêmes droits d'accès que l'ancienne.

4.2. Données conservées dans les systèmes de contrôle d'accès : Les données conservées par l'entreprise concernant son système de contrôle d'accès comprennent : •
Données du titulaire de la carte : o Nom et prénom
Intitulé du poste, service,
adresse courriel, numéro d'immatriculation de
l'employé, numéro de téléphone portable
• Cartes attribuées au titulaire
• Lieu, date et heure de l'opération de lecture de carte

4.2.1. Les données de contrôle d'accès peuvent être consultées par le personnel dont les fonctions requièrent l'accès au logiciel de contrôle d'accès. Ce personnel comprend :
• Agents de sécurité • Personnel technique chargé de délivrer les cartes d'accès ou d'effectuer les procédures de remplacement et de destruction des cartes
• Personnel de support technique informatique 4.2.2. Dans les cas où des données doivent être transférées du système de contrôle d'accès au destinataire demandeur,
Conformément aux procédures décrites dans la présente politique, dans la mesure du possible, tous les champs permettant d'identifier une personne physique doivent être supprimés. Par exemple, pour connaître le nombre d'utilisateurs d'un lecteur sur une période donnée, il ne sera pas nécessaire de divulguer les noms, photos ou autres informations personnelles des titulaires de carte dans le rapport ; seules les données relatives au processus de lecture seront transmises.

4.3. Méthodes de contrôle d'accès

L'accès aux données est assuré de différentes manières, selon les méthodes énumérées ci-dessous et en fonction des niveaux de classification des données.

Les méthodes de contrôle d'accès utilisées par défaut sont les suivantes :
• Ouvrez la connexion sur les appareils,
• Partage Windows et autorisations d'accès aux fichiers et dossiers,
• Restrictions des privilèges des comptes utilisateurs,

- droits d'accès au serveur et au poste de travail,
- autorisations du pare-feu,
- Listes de contrôle d'accès aux zones réseau et aux VLAN,
- Droits d'authentification intranet/extranet,
- Droits de connexion de l'utilisateur Kardelen Boya,
- Droits d'accès aux bases de données et listes de contrôle d'accès,
- Chiffrement des données au repos et en déplacement.
- Autres méthodes requises par le contrat par les parties concernées

4.4. Le contrôle d'accès s'applique à tous les réseaux, serveurs et postes de travail appartenant à Kardelen Boya. Cela s'applique aux ordinateurs portables et aux appareils mobiles.

4.5. Le contrôle d'accès basé sur les rôles sera utilisé comme méthode pour sécuriser l'accès à toutes les ressources basées sur des fichiers situées dans les domaines Active Directory de Kardelen Boya.

4.6. Tests d'intrusion : Le système de contrôle d'accès de Kardelen Boya fera l'objet de tests d'intrusion réguliers afin d'évaluer l'efficacité des contrôles existants et d'identifier toute faille. Le cas échéant et après accord, ces tests incluront également les systèmes des fournisseurs de services cloud.

POUR TOUTE DEMANDE RELATIVE AUX DONNÉES DE CONTRÔLE D'ACCÈS

FLUX DE PROCESSUS ACTUEL