[Nom de l'entreprise] Ltd
Politique de gestion d'actifs IS04
Aux exigences de l'ISO 27001:2017

Réf. document :	Politique de gestion d'actifs IS04
Version:	1
Date de la version:	[dd/mm/yyyy]
Auteur:	[Nom 1]
Approuvé par :	[Nom 2]
Niveau de	Contrôlé : Non contrôlé s'il est imprimé

confidentialité:	

Liste de circulation

Cette politique de gestion d'actifs est un document contrôlé et est maintenu sur le serveur comme lu uniquement. Le représentant de la gestion de la sécurité de l'information doit s'assurer que toutes les modifications sont distribuées et que les copies désuètes sont supprimées et déposées. Les copies papier utilisées pour la formation et la vérification interne sont contrôlées et distribuées comme suit.

Copie No.	**Holder**
1 Représentant en	gestion de la sécurité de l'information

Historique de l'amendement

Ce document est examiné périodiquement, au moins annuellement, et est conservé pour une période de [nombre] d'années. Les modifications et révisions sont distribuées aux titulaires nommés. L'historique des amendements et la question des révisions sont consignés ci-dessous.

Date	Amende. Non.	Page No.	Nouveau numéro no.	Raison du changement	Autorisé par
[dd/mm/yyyy]	-	Tous	1	Libération initiale.	[Nom 2]
	1		2		
	2		3		
	3		4		
	4		5		
	5		6		
	6		7		
	7		8		
	8		9		
	9		10		
	10		11		
	11		12		
	12		13		
	13		14		
	14		15		
	15		16		
	16		17		

Les copies de ce document autres que celles énumérées ci-dessus ne seront pas révisées; ces copies seront marquées comme non **contrôlées**.

Tableau des matières

0. Contrôles appliqués

Réf de contrôle	Titre
A.6.2.1	Politique sur les appareils mobiles
A.8.1.1	Inventaire des actifs
A.8.1.2	Propriété d'actifs
A.8.1.3	Utilisation acceptable des actifs
A.8.2.1	Classification de l'information
A.8.2.2	Étiquetage de l'information
A.8.3.1	Gestion des supports amovibles
A.8.3.2	Élimination des médias
A.8.2.3	Gestion des actifs
A.11.2.1	Ossage et protection de l'équipement
A.11.2.2	Soutien aux services publics
A.11.2.3	Sécurité de câblage
A.11.2.4	Entretien de l'équipement
A.11.2.6	Sécurité de l'équipement et des biens à l'extérieur des locaux
A.11.2.7	Élimination de la sécurité ou réutilisation de l'équipement
A.11.2.5	Retrait d'actifs
A.12.5.1	Installation de logiciels sur les systèmes opérationnels
A.17.1.3	Vérifier, examiner et évaluer la continuité de la sécurité de l'information
A.18.1.3	Protection des dossiers
A.18.2.2	Conformité aux politiques et normes de sécurité

1. Introduction

[Nom de l'entreprise] Ltd reconnaît l'importance de veiller à ce que ses actifs soient identifiés, enregistrés et protégés. [Nom de l'entreprise] Ltd est consciente de s'assurer que tous les actifs

qu'elle gère et possède sont comptabilisés, entretenus et contrôlés par la mise en œuvre des meilleures pratiques, des mécanismes d'enregistrement, des processus et des procédures.

2. But

Le but de cette politique est de s'assurer que tous les actifs TIC de [Business Name] Ltd sont identifiés enregistrés et d'établir de bonnes pratiques professionnelles dans la maintenance, la protection et la classification de tous les actifs TIC [Business Name] Ltd.

[Nom de l'entreprise] Ltd classe les actifs comme :

- Systèmes d'information et d'information :
    - Bases
    - Fichiers de données
    - Documents hardcopy
    - Guides utilisateur
    - Matériel de formation
    - Politiques, procédures
    - Plans de continuité d'activité
    - Données financières
- Logiciel:
    - Applications
    - Logiciel système
    - Logiciel de développement
    - Logiciel s'œdant des services publics
- Physique:
    - Matériel informatique
    - Équipement de communication
    - Médias – stockage et enregistrement
    - Propriété et hébergement
- Services:
    - Communications
    - Services publics (alimentation, éclairage, contrôles environnementaux)
- Personnel:
    - Connaissances
    - Compétences
    - Expérience
- Intangibles:
    - Réputation

3. Portée

Cette portée de cette politique s'étend à tous les départements[Business Name] Ltd, employés, entrepreneurs, fournisseurs et agences partenaires qui utilisent ou qui sont responsables du développement, de la gestion et de la maintenance de tous les actifs TIC [Business Name] Ltd.

4. Énoncé de politique générale

Le Département informatique assume la « propriété proposée » dans le but de fournir une « entité » par laquelle la responsabilité de gestion approuvée peut être contrôlée pour tous les actifs d'information et de données sur les TIC pour le compte de [Business Name] Ltd. Tous les actifs TIC identifiés (y compris le matériel, les logiciels et les licences, etc.) doivent être enregistrés dans l'inventaire des actifs TIC de [Business Name] Ltd.

[Nom de l'entreprise] Ltd doit prendre les mesures suivantes pour s'assurer que tous les biens sont correctement identifiés, enregistrés et entretenus.

4.1 Systèmes d'information et d'information

Les données et les informations détenues et conservées par [Business Name] Ltd peuvent être stockées sous forme de disque dur dans des emplacements physiques, des systèmes de classement, des bureaux ou stockées électroniquement à l'aide de logiciels et de systèmes de sauvegarde électroniques.

Types d'actifs des systèmes d'information et d'information :

- **Bases de données** – L'accès à ces données ne doit être donné qu'aux employés autorisés et les journaux doivent être tenus pour enregistrer tous les accès et modifications apportées aux données détenues dans n'importe quel système de base de données
- **Fichiers de** données – L'accès à n'importe quel fichier de données doit être donné uniquement aux employés autorisés et les journaux doivent être tenus pour enregistrer tous les accès et modifications apportées aux données détenues dans les systèmes de base de données
- **Documents hardcopy** – Tous les documents de copie papier contenant des données sensibles et personnelles identifiables doivent être consultés, traités, conservés et stockés en toute sécurité conformément aux directives d'information de [Business Name] Ltd. Les documents de copie papier restreints nécessitant un accès contrôlé doivent faire tenir un dossier de signature ou de sortie, le cas échéant.
- **Guides** d'utilisation – Tous les guides d'utilisateurs qui aident et aident à la compréhension des processus, des procédures ou des systèmes doivent être stockés en toute sécurité et devraient être facilement et facilement accessibles à tous les employés concernés – dans la mesure du possible. Les guides qui n'existent que sous forme physique devraient être numérisés pour inclure une version électronique qui peut être stockée électroniquement sur le réseau TIC de [Business Name] Ltd et diffusée dans la mesure du possible sur l'intranet de [Business Name] Ltd.
- **Matériel de** formation – Tout le matériel de formation pertinent doit être entreposé et facilement accessible à tous les employés concernés. La duplication ou la reproduction physique des manuels d'entraînement doit être maintenue au minimum et évitée dans la mesure du possible.

- **Politiques, procédures – Toutes les politiques et procédures** [business name] Ltd devraient être mises à disposition et diffusées via intranet [Business Name] Ltd – Toutes les copies originales des documents sur les politiques et procédures, qu'elles soient stockées ou en toute sécurité, examinées régulièrement et qu'un enregistrement de contrôle des antécédents de version soit conservé pour chaque document afin de s'assurer qu'ils sont à jour.
- **Plans de continuité** d'activité – Tous les plans de continuité d'activité doivent être régulièrement examinés, diffusés aux employés appropriés et stockés en toute sécurité pour faciliter la récupération au besoin.
- **Données financières** – Les données et informations relatives aux données financières [Business Name] Ltd doivent être réservées aux employés autorisés. Des mécanismes d'enregistrement doivent être mis en place pour l'accès à l'enregistrement, les modifications et l'utilisation des données et de l'information financières.

4.2Software

Les logiciels informatiques et informatiques sont largement utilisés dans [Business Name] Ltd et sont essentiels au fonctionnement quotidien de [Business Name] Ltd et à la fourniture de services essentiels à ses clients.

L'utilisation de logiciels a continué de changer le fonctionnement de [Business Name] Ltd. Des investissements substantiels ont été réalisés dans les logiciels, ainsi que des coûts et des dépenses permanents tels que le soutien annuel des logiciels et des systèmes, l'octroi de licences et la formation du personnel.

- **Applications** – *Les logiciels utilisés par [Business Name] Ltd doivent être provenant de manière appropriée à l'aide des fournisseurs approuvés par [Business Name] Ltd) et doivent être évalués en fonction des besoins de l'entreprise, de l'adéquation, de l'efficience, de la facilité d'utilisation, de la rentabilité et de l'intégration dans les systèmes existants [Business Name] Ltd. Tous les logiciels approuvés pour utilisation par [Business Name] Ltd doivent être enregistrés sur la liste des logiciels approuvés (lien ci-dessous). Un nombre approprié de licences logicielles doit être acheté pour couvrir le volume d'utilisation et satisfaire aux exigences légales. Les supports logiciels doivent être stockés (physiquement et électroniquement) dans un emplacement sécurisé et centralisé (DML – Médiathèque définitive) ainsi que les codes d'installation logicielle et les numéros d'enregistrement. L'accès aux médias logiciels/DML par les employés doit être contrôlé et limité aux seuls employés autorisés. Un registre doit être conservé de toutes les installations de logiciels, des volumes de licences de documentation SLA et des références dans un emplacement centralisé (base de données) où l'accès n'est fourni qu'aux employés autorisés. Un système de dédicace/sortie doit être utilisé pour contrôler l'utilisation des supports physiques.
- **Logiciel système** – Les logiciels serveur/système tels que les systèmes d'exploitation doivent être évalués en fonction des besoins de l'entreprise, de l'adéquation, de l'efficacité, de la rentabilité et de l'intégration dans les systèmes existants [Business Name] Ltd. Les supports d'installation du système d'exploitation doivent être stockés dans un emplacement sécurisé et centralisé (DML) avec les codes d'installation. L'accès aux supports logiciels server/système par les employés doit être contrôlé et limité aux seuls employés autorisés. Un registre doit être conservé de toutes les installations de logiciels, des volumes de licences de documentation SLA et des références dans un emplacement centralisé (base de données) où l'accès n'est fourni qu'aux employés autorisés. Un système de dédicace/sortie doit être utilisé pour contrôler l'utilisation des supports physiques. Les sauvegardes des installations complètes du serveur et des systèmes doivent être effectuées régulièrement à des fins de

récupération après sinistre. L'installation, la configuration et la maintenance des logiciels server/système ne doivent être entreprises que par des employés formés et qualifiés pour ce faire.

- **Les logiciels** de développement – tels que les logiciels RAD (Rapid Application Development) pour le soutien des systèmes existants et pour le développement de solutions internes doivent suivre les mêmes processus d'approvisionnement et d'utilisation que pour les applications et les logiciels Server/systems. Les logiciels de développement ne doivent être utilisés que par les employés qui sont formés ou qui suivent une formation pour utiliser le logiciel de développement.

Tous les types de logiciels (à l'exception des mises à jour de sécurité de routine et des correctifs vérifiés par les éditeurs de logiciels) doivent passer par des procédures d'achat convenues et doivent être enregistrés dans la liste des logiciels approuvés ISFnn de [Business Name] Ltd.

4.3 Physique

[Nom de l'entreprise] Les actifs les plus visibles de Ltd sont ceux qui sont physiquement situés dans [Business Name] Ltd tels que les ordinateurs, les imprimantes et les téléphones, etc. Les bureaux et les bâtiments doivent également être considérés comme des actifs des TIC – fournissant un emplacement pour le logement et l'installation de l'infrastructure ict data and communications network de [Business Name] Ltd et des documents et informations stockés physiquement.

- **L'équipement** informatique – un grand nombre d'appareils informatiques – qui comprend des PDA, des ordinateurs portables, des moniteurs, etc., sont utilisés dans l'ensemble des ordinateurs [Business Name] Ltd. Sont l'un des articles d'équipement les plus coûteux et doivent faire l'objet de contrôles, de l'approvisionnement à l'élimination. [Nom de l'entreprise] Ltd doit être en mesure de suivre toutes les activités et l'utilisation relatives à tous les appareils informatiques [Business Name] Ltd en utilisant divers moyens tels que via le réseau informatique et / ou en utilisant des systèmes d'enregistrement tels que la connexion et l'out et d'autres mécanismes d'enregistrement tels. Tous les ordinateurs doivent se voir attribuer un numéro d'étiquette d'actif unique qui est enregistré par rapport au numéro de série et au modèle du fabricant qui ne doivent jamais être modifiés ou échangés avec un autre ordinateur. Chaque ordinateur doit avoir le numéro d'étiquette solidement situé et facilement visible sur son boîtier extérieur avec les gravures de sécurité standard [Nom d'entreprise] Ltd. Tout au long de sa vie, un ordinateur peut faire l'objet de mises à niveau matérielles, de nouvelles installations logicielles, de changements de configuration et de maintenance. Toutes ces activités doivent être enregistrées dans le système de gestion d'actifs TIC de [Business Name] Ltd, qui est maintenu et mis à jour par le Département informatique.
- **Équipement de** communication – Les téléphones mobiles, les téléphones IP de bureau sont des appareils de communication largement utilisés dans [Business Name] Ltd. D'autres dispositifs de réseau et de communication identifiés comme actifs comprennent les routeurs, les commutateurs, l'équipement de vidéoconférence, etc. Avec l'équipement informatique, ces appareils doivent se voir attribuer un numéro d'étiquette d'actif qui est solidement situé et facilement visible sur l'appareil. Tous les équipements de communication doivent être identifiés et enregistrés dans la base de données sur la gestion des actifs TIC
- **Stockage et enregistrement des** médias – Les médias tels que les CD/DVD, la bande magnétique, les disques durs flash/portables sont des atouts précieux parce qu'ils sont utilisés pour enregistrer et récupérer des informations et des données [Business Name] Ltd. La nature portable de ce type de média exige une utilisation responsable et le respect de toutes les politiques, procédures et processus [Business Name] Ltd qui sont en place pour la

protection de l'information et des données. Des mécanismes appropriés d'étiquetage et d'enregistrement devraient être mis en place pour assurer la sécurité et l'intégrité des médias - permettre le suivi des supports essentiels tels que les sauvegardes de données, par exemple les supports nécessaires à la restauration des données et des fichiers, doit être signé à partir d'un endroit sûr. Les supports portables doivent être utilisés conformément à la politique de cryptage de [Business Name] Ltd, aux procédures de sécurité des ordinateurs portables et des appareils mobiles et aux procédures de protection des données et de traitement des médias.

Tous les supports/périphériques physiques d'ordinateur, de communication et de stockage doivent passer par des procédures d'achat convenues et doivent être enregistrés dans la liste du matériel approuvé ISFnn de [Business Name] Ltd.

4.4 Services

- **Communications** – Il est essentiel que [Business Name] Ltd maintiend sa capacité à communiquer sous différentes formes. L'équipement de communication doit être maintenu et des processus, des politiques et des procédures clairs pour la prestation de ce service doivent être en place. Le courrier électronique est également un moyen de communication essentiel et, à ce titre, nécessite une infrastructure robuste et fiable pour permettre à [Business Name] Ltd de communiquer efficacement et de manière fiable, tant à l'interne qu'à l'externe.
- **Services publics (électricité, éclairage, contrôles environnementaux)** – Ces services sont des atouts car ils fournissent des exigences fondamentales pour que [Business Name] Ltd fonctionne de façon appropriée, sécuritaire et efficace. Il est essentiel que l'entretien et les inspections des biens soient effectués régulièrement et que les employés soient proactifs dans la déclaration des défauts, chaque fois qu'ils sont notés, à la division des services immobiliers de [Business Name] Ltd.

4.5 Personnel

[Nom de l'entreprise] Ltd ne peut fonctionner sans sa main-d'œuvre – c'est son plus grand atout. La prestation de bons services exige que les employés de [Business Name] Ltd aient les compétences, les connaissances et la capacité nécessaires pour travailler dans de nombreux domaines et ministères différents dans [Business Name] Ltd. Le nombre de fonctions uniques dans [Business Name] Ltd exige une base variée de connaissances et de compétences qui doit être appuyée par des processus de recrutement robustes, une prestation de formation appropriée et une bonne gestion de l'identification des compétences des employés, du placement au travail et de l'allocation.

- **Connaissances et** expérience – [Nom d'entreprise] Ltd dispose d'un grand bassin d'employés qui ont une vaste base de connaissances et d'expérience à tirer parti et est un atout précieux.
- **Compétences** – Tous les employés de [Business Name] Ltd doivent posséder les compétences et la capacité nécessaires pour faire leur travail.

4.6 Immatériels

- **Réputation** – [Business Name] Ltd est très consciente que la perception et la confiance des clients dans sa capacité à fournir des services efficaces et efficients sont de la plus haute importance. La réputation est un atout qui favorise la confiance et génère un soutien dans ce que [Business Name] Ltd tente d'atteindre. [Nom de l'entreprise] Ltd prend sa réputation au

sérieux et s'engage proactivement à élaborer des politiques et des procédures ainsi qu'une approche cohérente dans le maintien et la présentation de la bonne image.

4.7 Classification de l'information

[Nom de l'entreprise] Ltd doit élaborer un système de classification de l'information par lequel tous les actifs liés aux TIC sont évalués et marqués pour indiquer le niveau de critique et de sensibilité. La classification consiste à regrouper l'information et à catégoriser le contenu afin d'établir le moyen le plus approprié de stockage/récupération et de déterminer qui est autorisé à accéder à des informations et des données particulières. Il est recommandé que la « propriété » de ce processus soit le service informatique de [Business Name] Ltd.

5. Responsabilités

Tous les départements, employés, entrepreneurs, fournisseurs et agences partenaires [Business Name] Ltd doivent respecter et respecter toutes les politiques et procédures d'utilisation acceptable relatives à tous les actifs TIC [Business Name] Ltd.

6. Violations de la politique

Les infractions à cette politique et/ou à ces incidents de sécurité peuvent être définies comme des événements qui auraient pu ou auraient entraîné des pertes ou des dommages aux actifs de [Business Name] Ltd, ou un événement qui contretait les procédures et les politiques de sécurité de [Business Name] Ltd.

Tous les employés [de Business Name] Ltd, les organismes partenaires, les entrepreneurs et les fournisseurs ont la responsabilité de signaler les incidents de sécurité et les violations de cette politique le plus rapidement possible par le biais de la procédure de déclaration des incidents de [Business Name] Ltd. Cette obligation s'étend également à toute organisation externe sous contrat pour soutenir ou accéder aux systèmes d'information de [Business Name] Ltd.

[Nom de l'entreprise] Ltd prendra les mesures appropriées pour remédier à toute violation de la politique et de ses procédures et lignes directrices connexes au moyen des cadres pertinents en place. Dans le cas d'une personne, l'affaire peut être traitée dans le cadre du processus disciplinaire.

7. Documents et documents associés

Document / Nom de l'enregistrement	Emplacement de stockage	Propriétaire	Contrôle de protection	Calendrier de rétention
Inventaire des actifs TIC isfnn	[Emplacement du lecteur]	[Nom 2]	Contrôlé : Accès protégé par mot de passe	[Heure]
Liste des logiciels approuvés par l'ISFnn	[Emplacement du lecteur]	[Nom 2]	Contrôlé : Accès protégé par mot de passe	[Heure]
Liste du matériel approuvé par l'ISFnn	[Emplacement du lecteur]	[Nom 2]	Contrôlé : Accès protégé par mot de passe	[Heure]

8. Gestion des documents

Ce document est valide à partir de [dd/mm/yyyy].

Ce document est examiné périodiquement et au moins annuellement afin d'assurer le respect des critères prescrits suivants.

- Conformité aux exigences de l'ISO 27001:2017
- Exigences législatives définies par la loi, le cas échéant

Directeur
[Nom 2]

_____
[Signature]