ARBONIA

IT SECURITY

Information Security Policy

Directive relative aux mots de passe

Version:	1.0
Votée:	08/07/2021
Statut:	RELEASED
Classification:	RESTRICTED
Auteur:	ICT Security Officer
Votée par:	Arbonia IT Board
Directive:	IS-ISP-GROUP-001-PASSWORD-POLICY_FR
Révision:	n/a

Informations relatives à la directive

Objectif	La directive relative aux mots de passe décrit et définit les principes s'appliquant à la création, à la gestion et à l'utilisation des mots de passe au sein du groupe Arbonia.
Utilisateurs/destinataires	▪ Tous les collaborateurs du groupe Arbonia ▪ Contractants externes/prestataires de services/clients et partenaires ayant accès aux systèmes TIC du groupe Arbonia
Enregistrement électronique des documents	https:\\security.arbonia.com

Justificatif de modification

Version	Date	Statut	Modification	par
0.1	2021-06-14	Draft	Draft of the policy	ICT Security Officer
0.9	2021-07-07	Draft	Draft for adoption	ICT Security Officer
0.9	2021-07-07	Review		Arbonia IT Board
1.0	2021-07-08	Adoption		Arbonia IT Board

Table des matières

Table des abréviations

Concept	Description
TIC	Informations and Communications Technology (technologies de l'information et de la communication)
OS	Operating System (système d'exploitation)
ISMS	Système de gestion de la sécurité des informations

Glossaire

Concept	Description
Attaque Brute Force	Une attaque Brute Force est la tentative de pirater un mot de passe ou un nom d'utilisateur en essayant toutes les possibilités.
Système de gestion de la sécurité des informations	Un système de gestion de la sécurité des informations consiste à établir des procédures et des règles au sein d'une organisation qui servent à définir, gérer, contrôler, maintenir et améliorer en permanence la sécurité des informations.

1 Objet, domaine d'application et utilisateurs

La directive décrit les exigences en matière de mot de passe et les consignes pour l'accès aux systèmes de TIC du groupe Arbonia. Elle définit les règles pour une gestion, une utilisation et la création sécurisées des mots de passe.

La directive s'applique à la totalité du domaine d'application du système de gestion de la sécurité des informations (ISMS), c'est-à-dire pour tous les systèmes de TIC du groupe Arbonia.

Les utilisateurs et destinataires de la présente directive sont tous les collaborateurs du groupe Arbonia ainsi que les contractants externes/prestataires de services/clients/partenaires etc. ayant besoin d'un accès aux systèmes TIC du groupe Arbonia.

2 Principes de gouvernance

2.1 Importance des mots de passe

La sécurité des systèmes de TIC d'Arbonia est fondée, entre autres, sur le soin avec lequel sont gérés les mots de passe et avant tout, comment les principes de base de l'utilisation des mots de passe sont suivis.

Un des principaux objectifs des hackers est le vol des données de connexion d'un utilisateur pour se procurer un accès aux systèmes de TIC du groupe Arbonia puis trouver et exploiter d'éventuelles lacunes. Ils tentent d'obtenir les autorisations privilégiées d'un administrateur système, avec lesquelles ils peuvent, dans le pire des cas, mener diverses activités telles que le vol de données, l'espionnage ou l'installation de logiciels malveillants sans se faire remarquer. C'est pourquoi les mots de passe faibles ainsi qu'une mauvaise manipulation de ceux-ci constituent un risque important. Ce risque est encore accru par l'utilisation d'autorisations privilégiées, qui sont souvent nécessaires pour réaliser les activités professionnelles.

C'est pourquoi il est impératif de lutter contre tout vol de données d'accès et de respecter les obligations suivantes.

2.2 Obligations des utilisateurs/propriétaires des comptes

Tous les utilisateurs doivent appliquer des procédures éprouvées et sécurisées pour la sélection et l'utilisation des mots de passe (plus de détails au chapitre 3):

- Il faut toujours choisir un mot de passe «fort». La longueur et le format d'un mot de passe doit être choisie de façon à rendre une attaque «brute force» fastidieuse et à la faire échouer.
- Les mots de passe ne doivent pas être communiqués à des tiers. Ceci s'applique également pour les supérieurs hiérarchiques, la direction et les administrateurs système.
- Les mots de passe ne doivent pas être écrits ou enregistrés de manière non conforme (par ex. dans Excel), à moins que le service informatique n'ait autorisé une méthode sécurisée prévue à cet effet (par ex. un outil de gestion des mots de passe).
- Le mot de passe doit être modifié à intervalles réguliers.
- Les mots de passe doivent être modifiés au moindre signe montrant qu'ils ont été rendus accessibles publiquement, c'est-à-dire à des tiers.
- Tout signe d'une utilisation abusive doit être immédiatement signalé au service informatique en charge.
- Si un(e) utilisateur(trice) dispose d'un compte utilisateur dédié avec des privilèges administratifs, n'utilisez pas le même mot de passe que le compte standard.
- Le titulaire du compte est dans tous les cas responsable du respect de la politique relative aux mots de passe, même si celle-ci n'est pas forcée techniquement. N'utilisez en aucun cas des mots de passe standard, vides ou faibles.

3 Directive relative aux mots de passe

3.1 Définitions

Afin d'atteindre un niveau approprié de sécurité des informations, différentes politiques relatives aux mots de passe sont appliquées en fonction des privilèges nécessaires. On différencie:

- l'utilisation générale de type «utilisateur», sans privilèges d'administrateur sur les systèmes de TIC,
- l'utilisation spécifique de type «administrateur», avec privilèges d'administrateur sur un ou plusieurs systèmes de TIC. Dans les comptes utilisateur de type «administrateur», on distingue:
    - les comptes de service/de système/de maintenance (utilisés pour les fonctions automatisées, l'installation ou la gestion des composants des systèmes de TIC tels que les OS, les bases de données, les applications ou les comptes de réseau etc.)
    - les comptes administrateur (utilisés pour les individus pour permettre leurs autorisations privilégiées au sein des systèmes de TIC)

3.2 Gestion des mots de passe

1. Le mot de passe est affecté à un identifiant de compte univoque (utilisateur ou administrateur)
2. Comme l'identifiant de compte, le mot de passe est personnel. Le mot de passe est connu uniquement de la personne responsable.
3. Le mot de passe ne doit pas être enregistré en texte clair.
4. La durée de validité du mot de passe ne doit jamais dépasser 360 jours ou 540 jours (voir chapitre 3.3)
5. Un nouveau mot de passe sera refusé s'il figure parmi les cinq derniers mots de passe utilisés.
6. Le nombre des échecs de saisie de mot de passe est limité à six. Après la sixième tentative, le compte est verrouillé jusqu'à ce qu'un administrateur le débloque.
7. Le compteur des tentatives de connexion échouées ne doit pas être réinitialisé en moins de 60 minutes
8. Les mots de passe temporaires doivent avoir une validité <72 h et une requête doit exiger de l'utilisateur, lors de la première connexion, qu'il modifie le mot de passe temporaire. Ceci s'applique dans la mesure des possibilités techniques. Dans le cas contraire, chaque détenteur de compte est personnellement responsable de cette modification de mot de passe.
9. L'attribution automatique du mot de passe lors de l'ouverture d'un compte utilisateur est effectuée selon les mêmes spécifications.

Règles spéciales pour les comptes de service/de système/de maintenance:

- Exception à la règle n° 2: les mots de passe liés à ce type de compte peuvent être conservés dans un outil de gestion des mots de passe sécurisé (crypté) avec accès protégé par mot de passe et partagés avec plusieurs personnes au moyen de groupes définis de rôles et d'autorisations, dans la mesure ou ceci est nécessaire à l'exécution de leur activité
- Exception à la règle n° 4: les mots de passe liés à ce type de compte, si nécessaire, peuvent disposer de l'activation de l'option de non-péremption des mots de passe
- Exception à la règle n° 6: les mots de passe liés à ce type de compte ne sont pas soumis à la nécessité du verrouillage automatique

La gestion des exceptions est traitée au chapitre 3.5.

3.3 Consignes relatives aux mots de passe

Le mot de passe pour un compte de type «**utilisateur**», **sans** privilèges d'administrateur sur les systèmes de TIC doit répondre aux exigences suivantes:

- contient au moins 12 caractères pour une validité du mot de passe de 360 jours ou au moins 16 caractères pour une validité du mot de passe de 540 jours
- présente une complexité de 4 sur 4, c'est-à-dire que les caractères suivants doivent être utilisés respectivement au moins une fois:
    - lettres majuscules
    - lettres minuscules
    - chiffres de 0–9
    - signes de ponctuation ou caractères spéciaux (tous les systèmes de TIC n'acceptent pas tous les caractères)
- ne doit pas contenir le nom de compte
- ne doit pas contenir de chiffres en première et dernière position
- ne doit pas contenir trois caractères identiques consécutifs

Le mot de passe pour un compte de type «**administrateur**», **avec** privilèges d'administrateur sur les systèmes de TIC doit en outre respecter les règles spéciales suivantes:

Règles spéciales pour les comptes de service/de système/de maintenance:

- contient au moins 32 caractères
- le mot de passe doit être généré aléatoirement et documenté au moyen d'un outil de gestion des mots de passe approprié (voir l'exception à la règle n° 2, chapitre 3.2)

Règle spéciale pour les comptes d'administrateur:

- Contient au moins 15 caractères

Règles spéciales pour les systèmes tiers (B2C, B2B et autres) exploités par le groupe Arbonia:

Les consignes relatives aux mots de passe s'appliquent en principe également aux systèmes tiers, peuvent néanmoins être adaptées au Business Use Case respectif si cela s'avère nécessaire. Dans tous les cas, les règles spéciales doivent faire l'objet d'un traitement selon le chapitre 3.5.

Consignes spéciales pour les comptes Windows – internes à Arbonia et appliquées automatiquement:

- Le nouveau mot de passe ne doit pas être présent dans une base de données de mots de passe compromis. Un contrôle technique lors de la création du mot de passe l'empêche.
- Le nouveau mot de passe ne doit pas figurer dans un dictionnaire personnalisé. Ce dictionnaire fait l'objet d'une gestion centrale et contient, entre autres, le nom de la société. Les mots non autorisés sont directement affichés en cas de correspondance.
- Le mot de passe doit être modifié s'il apparaît dans une base de données de mots de passe compromis.

3.4 Stratégie en matière de mots de passe

Historique des mots de passe	5
Durée de validité maximale du mot de passe	360 jours (12–15 caractères) ou 540 jours (≥16 caractères)
Durée de validité minimum du mot de passe	0
Complexité	4/4 (lettres en majuscules/en minuscules/chiffres de 0–9/signes de ponctuation ou caractères spéciaux)
Longueur minimale du mot de passe o Utilisateur o Comptes de service/de système/de maintenance o Comptes d'administrateur	 12 caractères 32 caractères (génération aléatoire) 15 caractères
Cryptage inversé (domaine Windows)	désactivé
Nombre de tentatives de connexion échouées jusqu'à ce que le compte soit bloqué	6
Durée de blocage du compte	Jusqu'au déverrouillage par un administrateur
Durée avant que le compteur de tentatives de connexion échouées ne soit réinitialisé	≥ 60 minutes
Spécificités (domaine Windows)	Le mot de passe ne doit pas contenir de chiffres en première et dernière position. Le mot de passe ne doit pas contenir trois caractères identiques consécutifs.

3.5 Exceptions/Spécificités

Tous les procédés d'authentification informatiques doivent, dans la mesure du possible, mettre en œuvre les consignes de la présente directive et contrôler le respect de celles-ci. Si des conditions techniques nécessaires à l'implémentation ne sont pas données, celles-ci doivent être assurées par le détenteur du compte, au moyen d'un processus manuel, et un mot de passe fort, dans le cadre des possibilités du système, doit être utilisé.

Le responsable de la sécurité informatique local peut établir des autorisations d'exception relatives à la présente directive, si les principes de la sécurité des informations sont respectés et s'il n'existe aucun risque pour les systèmes de TIC du groupe Arbonia. Il décide, si nécessaire après avoir consulté le responsable de la sécurité des TIC, de l'octroi d'une exception ou définit des mesures complémentaires pour minimiser le risque. Toutes les exceptions doivent être consignées par écrit dans un répertoire.

4 Création de mots de passe forts

Il existe différentes techniques pour créer un mot de passe fort et s'en souvenir:

Exemple 1: former un mot de passe fort sur la base d'une phrase

Sélectionnez une phrase dont vous vous souviendrez facilement et transformez-la en mot de passe.

Ex. : Il n'est pas si dur de choisir un mot de passe fort.

Utilisez la lettre initiale ou plusieurs lettres des différents mots et enrichissez le mot de passe avec des chiffres et des caractères spéciaux.

Ex. : In'epsddc1mdpf.

Exemple 2: former un mot de passe fort en remplaçant des caractères

Sélectionnez un mot dont vous pourrez vous souvenir facilement, par ex. «automobile» et définissez une suite de caractères spéciale, par ex. «1$1». Remplacez alors des parties/lettres définies du mot avec la suite de caractères spécifique pour obtenir un mot de passe fort.

Ex. : aut1$1m1$1bile

Attention à ne jamais utiliser pour la création de votre mot de passe des informations en accès libre sur les médias sociaux. D'autres astuces relatives à la sécurité des mots de passe sont communiquées lors des formations IT Security Awareness.

5 Documents de référence

- IS-ISS-GROUP-001-INFORMATION-SECURITY-STRATEGY
- IS-GISP-GROUP-001-GENERAL-INFORMATION-SECURITY-POLICY
- IS-SISD-GROUP-001-PSSS-SPECOPS
- Directive relative à l'utilisation des systèmes informatiques chez Arbonia

6 Entrée en vigueur

Nom	Unité	Fonction	Date	Signature
Patrick Langenegger	Corporate IT	CIO Arbonia Group / CIO Division Doors	2021-07-08	n/a
Michael Kreter	Division HVAC / Sanitary	CIO Division HVAC / Sanitary	2021-07-08	n/a
Tobias Shibli	Division Windows	CIO Division Windows	2021-07-08	n/a
Reto Knechtle	Corporate IT	Head of IT Infrastructure	2021-07-08	n/a

7 Annexes pertinentes

N°	Description	Nom du fichier
1	IS-ISP-GROUP-001-COM001-EMPLOYEE-INFORMATION	