ARBONIA

IT SECURITY

Information Security Policy

Política de palavras-passe

Versão:	1.0
Aprovado:	08.07.2021
Estado:	RELEASED
Classificação:	RESTRICTED
Elaborado por:	ICT Security Officer
Aprovado por:	Arbonia IT Board
Política:	IS-ISP-GROUP-001-PASSWORD-POLICY_PT
Revisão:	n/a

Informações sobre a política

Finalidade	A política de palavras-passe descreve e define os princípios para a criação, gestão e utilização de palavras-passe no grupo Arbonia Gruppe.
Utilizador/destinatário	▪ Todos os colaboradores do Grupo Arbonia ▪ Fornecedores externos/prestadores de serviços/clientes e parceiros que tenham acesso aos sistemas de TIC do Grupo Arbonia
Armazenamento eletrónico de documentos	https:\\security.arbonia.com

Histórico de alterações

Versão	Data	Estado	Alteração	por
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

Índice

Lista de abreviaturas

Termo	Descrição
TIC	Informations and Communications Technology (tecnologias de informação e comunicação)
SO	Operating System (sistema operativo)
SGSI	Sistemas de Gestão de Segurança da Informação

Glossário

Termo	Descrição
Ataque de força bruta	Um ataque de força bruta consiste na tentativa de decifrar uma palavra-passe ou nome de utilizador, experimentando todas as possibilidades.
Sistemas de Gestão de Segurança da Informação	Um sistema de gestão de segurança da informação pressupõe o estabelecimento de procedimentos e regras dentro de uma organização, que servem para definir, gerir, controlar, manter e melhorar continuamente a segurança da informação.

1 Finalidade, âmbito de aplicação e utilizador

A política descreve os requisitos e as instruções de palavras-passe para o acesso aos sistemas TIC do Grupo Arbonia. Estabelece regras para a gestão, utilização e criação de palavras-passe seguras.

A política aplica-se a todo o âmbito do Sistema de Gestão de Segurança da Informação (SGSI), ou seja, a todos os sistemas TIC do Grupo Arbonia.

Os destinatários desta política são todos os colaboradores do Grupo Arbonia, bem como fornecedores externos/prestadores de serviços/clientes/parceiros e outros que necessitem do acesso aos sistemas de TIC do Grupo Arbonia.

2 Princípios de governança

2.1 Importância das palavras-passe

A segurança dos sistemas de TIC da Arbonia baseia-se, entre outras coisas, no cuidado com que as palavras-passe são tratadas e, acima de tudo, na observância dos princípios básicos de utilização de palavras-passe.

Um dos principais objetivos dos autores dos ataques é roubar as credenciais de um utilizador para ter acesso aos sistemas de TIC do Grupo Arbonia e depois encontrar e explorar eventuais pontos fracos. Tentam apropriar-se das permissões de um administrador de sistema, que lhes permitam, no pior dos casos, realizar várias atividades como o roubo de dados, espionagem ou instalação de malware, sem que sejam detetados. Por esta razão, as palavras-passe fracas, bem como a gestão incorreta, representam um risco considerável. Este risco aumenta ainda mais com a utilização requerida de permissões, que são frequentemente necessárias para o exercício da atividade profissional.

É por isso imperativo prevenir o roubo de dados de acesso e observar os seguintes deveres.

2.2 Deveres dos utilizadores/titulares da conta

Todos os utilizadores devem respeitar as melhores e mais seguras práticas na escolha e utilização de palavras-passe (ver capítulo 3 para mais detalhes):

- Deve sempre ser escolhida uma palavra-passe «forte». O comprimento e o formato de uma palavra-passe devem ser escolhidos de modo a que um ataque de força bruta seja demorado e não conduza ao sucesso
- As palavras-passe não devem ser reveladas a terceiros, nem a supervisores, gestores ou administradores de sistemas
- As palavras-passe não devem ser anotadas ou indevidamente armazenadas (por ex. em Excel), a menos que o departamento de TI tenha aprovado um método seguro (por ex. uma ferramenta de gestão de palavras-passe) para o efeito.
- A palavra-passe deve ser alterada em intervalos regulares
- As palavras-passe devem ser alteradas se houver indícios de que tenham sido disponibilizadas ao público, ou seja, a terceiros
- Os indícios de utilização indevida devem ser comunicados de imediato ao respetivo departamento de TI
- Se um/a utilizador/a possuir uma conta de utilizador dedicada com privilégios de administrador, não deve ser utilizada a mesma palavra-passe da conta normal.
- O titular da conta é sempre responsável pelo cumprimento da política de palavras-passe, mesmo que esta não seja um requisito técnico. Em caso algum deve ser utilizada uma palavra-passe por defeito, em branco ou fraca

3 Política de palavras-passe

3.1 Definição

Para atingir um nível adequado de segurança da informação, são aplicadas diferentes políticas de palavras-passe de acordo com os privilégios necessários. É feita a distinção entre:

- Utilização geral do tipo «Utilizador», sem privilégios de administrador em sistemas de TIC
- Utilização específica do tipo «Administrador», com privilégios de administrador em um ou mais sistemas de TIC. As contas de utilizadores do tipo «Administrador» distinguem-se por:
    - Contas de serviço/de sistema/de assistência (utilizadas para funções automatizadas, instalação ou administração de componentes em sistemas de TIC, tais como SO, bases de dados, aplicações ou contas de rede e outros)
    - Contas de administradores (utilizadas para indivíduos, para que lhes seja concedido o acesso privilegiado aos sistemas de TIC.)

3.2 Arbonia Management AG

1. A palavra-passe é atribuída a um único ID de conta (utilizador ou administrador)
2. Tal como o ID da conta, a palavra-passe também é pessoal. A palavra-passe só é do conhecimento da pessoa responsável.
3. A palavra-passe não deve ser guardada como texto simples
4. A validade da palavra-passe nunca deve exceder 360 dias ou 540 dias (ver capítulo 3.3)
5. Uma nova palavra-passe será recusada se for igual a uma das últimas 5 palavras-passe utilizadas
6. O número de tentativas falhadas de introdução da palavra-passe está limitado a 6. Após a sexta tentativa, a conta será bloqueada até que um administrador a desbloqueie novamente.
7. O contador de tentativas de início de sessão falhadas não pode ser reposto em menos de 60 minutos
8. As palavras-passe temporárias podem ter uma validade de <72 h e o utilizador deve ser alertado para alterar a palavra-passe temporária aquando do primeiro início de sessão. Este princípio aplica-se na medida em que seja tecnicamente viável. Caso contrário, cada titular de conta é responsável por esta alteração da palavra-passe
9. A atribuição automática de palavras-passe aquando da abertura de uma conta de utilizador é efetuada de acordo com as mesmas instruções

Requisitos específicos para contas de serviço/de sistema/de assistência:

- Exceção à regra n.º 2: As palavras-passe associadas a este tipo de conta podem ser guardadas numa ferramenta segura (encriptada) de gestão de palavras-passe, com acesso protegido por palavra-passe, e partilhadas com várias pessoas através de grupos de funções e permissões definidos, na medida em que seja necessário para o desempenho das suas funções
- Exceção à regra n.º 4: Se necessário, as palavras-passe associadas a este tipo de conta devem ter ativada a opção de nunca expirarem
- Exceção à regra n.º 6: As palavras-passe associadas a este tipo de conta não devem ser bloqueadas automaticamente

As exceções encontram-se descritas no capítulo 3.5.

3.3 Instruções para palavras-passe

A palavra-passe de uma conta do tipo **«Utilizador» sem** privilégios de administrador em sistemas de TIC devem preencher os seguintes requisitos:

- Conter pelo menos 12 caracteres para uma validade de 360 dias ou pelo menos 16 caracteres para uma validade de 540 dias
- Possuir uma complexidade de 4 em 4, o que significa que os seguintes caracteres devem ser utilizados pelo menos uma vez:
    - Maiúsculas
    - Minúsuculas
    - Dígitos 0–9
    - Sinais de pontuação ou caracteres especiais (nem todos os sistemas de TIC aceitam todos os caracteres)
- Não deve incluir o nome da conta
- Não deve incluir dígitos na primeira e na última posição
- Não deve conter 3 caracteres idênticos consecutivos

As palavras-passe de uma conta do tipo **«Administrador» com** privilégios de administrador em sistemas de TIC estão sujeitas aos seguintes requisitos específicos:

Requisitos específicos para contas de serviço/de sistema/de assistência:

- Conter pelo menos 32 caracteres
- A palavra-passe deve ser gerada aleatoriamente e documentada através de uma ferramenta de gestão de palavras-passe adequada (ver excepção à regra nº 2, capítulo 3.2)

Requisito específico para contas de administradores:

- Conter pelo menos 15 caracteres

Requisito específico para sistemas de terceiros (B2C/B2B e outros) que sejam explorados pelo Gupo Arbonia:

Por norma, as instruções para palavras-passe aplicam-se igualmente a sistemas de terceiros, mas podem ser adaptadas ao Business Use Case, se necessário. Em todo o caso, os requisitos específicos devem ser tratados de acordo com o capítulo 3.5.

Instruções específicas para contas do Windows – aplicadas internamente pela Arbonia e automaticamente:

- A nova palavra-passe definida não deve constar numa base de dados com palavras-passe comprometidas. Uma verificação técnica aquando da definição da palavra-passe impede que isto aconteça
- A nova palavra-passe definida não deve constar num dicionário definido pelo utilizador. Esse dicionário é gerido a nível central e contém, entre outras coisas, o nome da empresa. As palavras proibidas são exibidas diretamente em caso de coincidência
- A palavra-passe deve ser alterada se constar numa base de dados com palavras-passe comprometidas

3.4 Estratégia de palavras-passe

Histórico de palavras-passe	5
Validade máxima da palavra-passe	360 (12–15 caracteres) ou 540 dias (≥16 caracteres)
Validade mínima da palavra-passe	0
Complexidade	4/4 (maiúsculas/minúsculas/dígitos 0–9/sinais de pontuação ou caracteres especiais)
Comprimento mínimo da palavra-passe o Utilizador o Contas de serviço/de sistema/de assistência: o Contas de administradores	 12 caracteres 32 caracteres (gerada aleatoriamente) 15 caracteres
Encriptação inversa (domínio Windows)	desativado
Número de tentativas de início de sessão falhadas até que a conta seja bloqueada	6
Duração do bloqueio da conta	Até um administrador a desbloquear
Duração até à reposição do contador de tentativas de início de sessão falhadas	≥ 60 minutos
Casos específicos (domínio Windows)	A palavra-passe não deve incluir dígitos na primeira e na última posição A palavra-passe não deve conter 3 caracteres idênticos consecutivos

3.5 Exceções / casos específicos

Todos os procedimentos de autenticação baseados em sistemas informáticos devem, na medida do possível, implementar e verificar a conformidade com as instruções da presente política. Se faltarem requisitos técnicos de implementação, estes devem ser assegurados através de um processo manual pelo respetivo titular da conta e deve ser utilizada uma palavra-passe forte dentro do âmbito das opções do sistema.

O responsável local pela segurança das TI pode conceder exceções à presente política, desde que sejam observados os princípios de segurança da informação e não exista risco para os sistemas de TIC do Grupo Arbonia. Este decide, se necessário, em consulta com o coordenador de segurança TIC, se deve conceder uma exceção ou definir outras medidas para minimizar o risco. Todas as exceções devem ser registadas por escrito numa pasta.

4 Criação de palavras-passe fortes

Existem várias técnicas para criar e decorar uma palavra-passe forte:

Exemplo 1: Criar uma palavra-passe forte com base numa frase

Escolha uma frase de que se recorde bem e transforme-a numa palavra-passe.

Ex.: Não é assim tão difícil, escolher uma palavra-passe forte.

Utilize a primeira letra ou várias letras de cada palavra e fortaleça a palavra-passe com dígitos e caracteres especiais.

Ex.: Néatd,e1P-pf.

Exemplo 2: Criar uma palavra-passe forte substituindo os caracteres

Escolha uma palavra de que se recorde bem, por ex. «Automóvel» e defina uma sequência especial, por ex. «1$1». Agora substitua as partes/letras definidas da palavra pela sua sequência especial para obter uma palavra-passe forte.

Ex. Aut1$1m$1$vel

Tenha em atenção que nunca deve utilizar informações que estejam livremente acessíveis nas redes sociais para criar a sua palavra-passe. Pode obter mais dicas sobre o tema da segurança das palavras-passe nos nossos cursos de formação de sensibilização para a segurança em TI.

5 Documentos de referência

- IS-ISS-GROUP-001-INFORMATION-SECURITY-STRATEGY
- IS-GISP-GROUP-001-GENERAL-INFORMATION-SECURITY-POLICY
- IS-SISD-GROUP-001-PSSS-SPECOPS
- Política para a utilização de sistemas de TI na Arbonia

6 Entrada em vigor

Nome	Unidade de negócios	Cargo	Data	Assinatura
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 Anexos relevantes

N.º	Descrição	Nome do ficheiro
1	IS-ISP-GROUP-001-COM001-EMPLOYEE-INFORMATION	