Política para a Segurança da Informação Digital

Esta política responde aos standards ISO 9001 e ISO 27001

Aplica-se a Todos os Colaboradores/Funcionários Internos e Externos

Municipio de Olhão

Aprovado em Reunião de Câmara a 11-01-2023

município de Olhão ...mais para si!	Adaptado da Política Regional, proposta pelo grupo de trabalho TI e consultores da Região de Aveiro e aprovada pelo conselho intermunicipal.

Convidamos todos os Colaboradores

a contribuir para garantir a

Segurança e Privacidade de toda a Informação pertencente à Organização e aos Cidadãos.

Obrigado pela sua colaboração!

São esperadas do Colaborador as seguintes Boas Práticas:

- Melhorar a atitude e o comportamento responsável;
- Conhecer as Regras de Segurança em detalhe;
- Cumprir as Regras e Boas Práticas;
- Contribuir e propor melhorias;
- Divulgar, Informar e Sensibilizar os Colegas;
- Comunicar qualquer não cumprimento, com vista à sua correção.

«A melhor defesa e segurança é o seu adequado comportamento em cada dia»

Índice

Capítulo 1 - Termos e Condições

1. Referências que orientam esta Política

x Regulamento (UE) 2016/679 RGPD

O seguimento desta Política por todos os Colaboradores é essencial para reduzir o risco de quebras de segurança na privacidade da informação dos Cidadãos.

x Resolução do Conselho de Ministros n.º 41/2018

Esta Política incorpora os requisitos técnicos obrigatórios.

x Norma ISO 2001 – Sistema de Gestão da Qualidade

Demonstração da capacidade da organização em satisfazer as necessidades dos Cidadãos de acordo com a regulamentação aplicável. Esta Política é uma componente essencial da responsabilidade da área TI.

x Norma ISO 27001 – Sistema de Gestão da Segurança da Informação

Esta Política é uma componente base essencial para assegurar a Segurança da Informação.

2. Glossário – Termos e Conceitos

Este ponto foi propositadamente colocado em primeiro lugar para o melhor entendimento do sentido em que são utilizados os seguintes termos neste documento.

Política	Conjunto de Regras e Procedimentos que deve ser seguido pelos Colaboradores para garantir os fins de utilização Segura e Responsável dos Sistemas Digitais da Organização.
Colaborador	Utilizador dos Sistemas Digitais da Organização. Inclui Colaboradores Internos, Autarcas e pessoas externas prestadoras de serviços. O termo Colaborador foi escolhido porque ser mais amplo e ter um significado mais atual, sublinhando a importância central do comportamento humano para o sucesso da Organização e o cumprimento de regulamentos, tais como RGPD.

Sistemas Digitais	Qualquer Equipamento digital informático, solução de software, plataforma de serviço, site, rede ou canal de comunicações digitais. Foi escolhida esta designação como genérica. Dependendo da regra representa um ou mais elementos antes listados.
Perfil	Conjunto de características ou competências necessárias ao desempenho de uma atividade, cargo ou função.
Organização	Conjunto de pessoas que tem as suas próprias funções com responsabilidades, autoridades e relações para atingir os objetivos do Município de Olhão.

3. Âmbito e Descrição

Esta Política define as boas práticas para a utilização segura dos sistemas de informação digitais e assegurar as melhores condições de trabalho aos colaboradores para a prestação de serviços aos Cidadãos.

4. A quem se aplica

Esta política aplica-se a todos os Colaboradores internos e externos da Organização, sempre que utilizem ou tenham acesso a qualquer sistema ou informação digital propriedade da organização.

«Obrigado pela sua colaboração. A melhor defesa e segurança é o seu comportamento responsável.»

5. Aceitação e validade

Esta Política é **mandatória**, deve ser respeitada por todos os Colaboradores e não carece de aceitação ou consentimento explícito.

Esta Política mantém-se em vigor permanentemente. Uma nova versão de Melhoria Contínua será publicada sempre que possível.

6. Autoridade

Esta Política foi aprovada pelo Presidente da Organização e é considerada da mais elevada importância.

7. Monitorização da utilização dos Sistemas Digitais

O Colaborador deve ter presente que será monitorizada, registada e rastreada toda a atividade de acesso aos Sistemas Digitais da Organização, à Internet e envio de correio eletrónico.

Este registo será utilizado para prevenir e identificar violações de segurança, políticas definidas ou qualquer atividade que possa pôr em risco o serviço da Organização.

8. Contacto para todos os assuntos sobre segurança da informação digital, esclarecimentos e comunicação de incidente de segurança

O Colaborador está obrigado a comunicar de imediato à Divisão de Informática qualquer incidente ou suspeita de incidente relacionado com segurança.

Procedimento: Enviar um mail para ciberseguranca@cm-olhao.pt com descrição do sucedido.

9. Contacto do Responsável pela Melhoria Contínua

Convidamos Todos os Colaboradores a contribuir para a melhoria contínua desta política.

Deve propor melhorias enviando mail para ciberseguranca@cm-olhao.pt com o assunto: Contributo para a melhoria da Política para a Segurança da Informação Digital

10. Comunicação, sensibilização e formação

Convidamos Todos os Colaboradores a contribuir para a melhoria contínua desta política.

Todos os Colaboradores que utilizem um sistema digital da organização têm a obrigação de conhecer, praticar e promover, as boas práticas de segurança.

Um novo Colaborador receberá formação de acolhimento sobre a política de segurança da organização.

Qualquer Colaborador é encorajado e pode pedir formação ou

esclarecimento adicional sobre a política de segurança da organização.

11. Histórico de Revisões

Data da Mudança	Responsável	Sumário de alterações
2022-11-22	DR	Primeira versão 1.0.

Capítulo 2 - REGRAS

As **REGRAS** apresentam-se agrupadas em 10 categorias.

O Colaborador deve ter presente que será monitorizada, registada e rastreada toda a atividade de acesso aos Sistemas Digitais da Organização, à Internet e envio de correio eletrónico. Este registo será utilizado para prevenir e identificar violações de segurança, políticas definidas ou qualquer atividade que possa pôr em risco o serviço da Organização.

Todas as regras e recomendações gerais comunicadas pela Organização aplicam-se a todos os Colaboradores qualquer que seja a atividade exercida.

1. Regras sobre OBRIGAÇÕES LEGAIS

O Colaborador poderá incorrer em procedimento interno ou em penalizações legais caso execute ações propositadas ou negligentes no âmbito das regras descritas em seguida.

É expressamente proibido ao Colaborador:

1.1. **Executar ações que prejudiquem** o bom funcionamento dos Sistemas de Informação da Organização;

1.2. **Divulgar informação sensível ou sigilosa**, incluindo informação acerca dos Sistemas de Informação da Organização;

1.3. **Utilizar para qualquer atividade ilícita** os sistemas digitais, equipamentos e redes de comunicação da Organização, nomeadamente, o acesso ilícito a qualquer sistema ou informação, interno ou externo;

1.4. **Tentar introduzir ou difundir propositadamente código malicioso** nos Sistemas de Informação e de Comunicações tal como: vírus, worm, trojan horse (cavalo de Troia), e-mail bomb, e-mail spam, spyware (software espião), adware (software de publicidade), keylogger (software registo de teclado) ou outro análogo;

1.5. **Violar os direitos legais de propriedade**, incluindo cópias indevidas de ficheiros e software violando a legislação em vigor ou regulamentos internos.

2. Regras sobre COMUNICAÇÃO DE INCIDENTES E QUEBRAS DE SEGURANÇA

O Colaborador está obrigado a comunicar de imediato à Divisão de Informática:

1. Enviando um mail para ciberseguranca@cm-olhao.pt
2. Ligando para a extensão 8313
3. Ligando para 289 700 106

2.1. **Qualquer Incidente** ou suspeita relacionados com possível **Quebra de Segurança**;

2.2. **Sempre que perca a posse ou controlo de qualquer equipamento** digital que contenha informação da Organização ou direitos de acesso aos Sistemas de Informação da Organização.

2.3. **DEVE comunicar imediatamente**, por escrito, à Divisão de Informática a perda ou furto de equipamentos, incluindo descrição total sobre a ocorrência. A Divisão de Informática ativará o procedimento de segurança adequado dependendo do relato efetuado pelo Colaborador.

3. Regras sobre SEGURANÇA DA INFORMAÇÃO

3.1. **O Colaborador é responsabilizado pelas ações** sobre a informação produzida e/ou modificada com recurso às credenciais de contas de utilizador que lhe foram atribuídas;

3.2. As autorizações de acesso serão solicitadas pelo gestor da informação em causa, em conformidade com as normas definidas pela Divisão de Informática. **O Colaborador não pode aceder a informação**, sistemas informáticos ou redes de comunicação, **aos quais não tenha autorização**;

3.3. **O Colaborador deve assegurar a privacidade da informação que utiliza e a que tiver acesso**. Não pode divulgar ou permitir a outra pessoa o acesso físico ou digital à informação da Organização, para qualquer fim que não seja adequado às boas práticas da Organização;

3.4. **Toda a informação em ficheiros é propriedade da Organização**. Os Documentos de trabalho armazenados e alterados pelo Colaborador no disco

local devem ser copiados, logo que possível, para a pasta adequada em servidor. A Divisão de Informática só se responsabiliza pela salvaguarda de Documentos/Ficheiros armazenados nos servidor.

3.5 **A informação considerada propriedade da organização não pode ser armazenada em equipamentos pessoais ou em ambientes não controlados** pela Divisão de Informática, incluindo recursos de organismos externos com quem a organização não tenha um contrato para o efeito.

4. Regras sobre UTILIZAÇÃO RESPONSÁVEL DOS RECURSOS INFORMÁTICOS

O Colaborador deve garantir a utilização responsável dos recursos informáticos (equipamentos digitais, software e comunicações) seguindo as seguintes orientações:

4.1 **DEVE evitar** utilizar os recursos informáticos **para qualquer outra finalidade que não seja ao serviço do interesse da Organização**, e ter sempre presente o bom senso;

4.2. **DEVE garantir a segurança e proteção contra terceiros** dos recursos que lhe estão atribuídos. **NÃO deve abandonar** recursos informáticos portáteis sem vigilância. **Deve** garantir que são guardados em local seguro;

4.3. **DEVE entregar** ao Serviço Responsável todos os recursos informáticos que tenha em sua posse, em caso de extinção ou suspensão do vínculo com o Município de Olhão. De igual modo, quando aplicável, em caso de Mobilidade para outro serviço ou localização, ou alteração para funções que não requeiram esses recursos.

5. Regras sobre UTILIZAÇÃO RESPONSÁVEL DA INTERNET E CORREIO ELECTRÓNICO

A Internet e o Correio eletrónico são recursos fornecidos pela Organização para facilitar as atividades de trabalho do Colaborador.

Todas as regras e recomendações gerais comunicadas pela Organização aplicam-se a todos os Colaboradores independentemente do vínculo e a atividade exercida.

A Organização reserva o direito de limitar através de regras o acesso à Internet e o conteúdo das mensagens de Correio Eletrónico recebidas e enviadas, por perfil funcional do Colaborador.

5.1.**O Colaborador responde pela utilização adequada do acesso à Internet e do Correio eletrónico**, e deve utilizar apenas de acordo com o âmbito e fins da respetiva atividade que lhe é pedida pela Organização.

5.2.**É proibida** a utilização da Internet, Correio eletrónico ou qualquer outro canal de comunicação que viole ou coloque em causa: as Políticas da organização, as Políticas de Segurança dos Sistemas de Informação, a Legislação em vigor, valores Éticos e Morais, a Imagem da Organização.

5.3.**É proibido** o acesso, utilização, download, envio ou reencaminhamento de mensagens e conteúdos impróprios e que não se relacionem com os interesses da Organização, tais como: Chat público, Hacking, Crime e Violência, Racismo e descriminação, Estupefacientes, Pornografia, Jogos, Filmes ou qualquer outro conteúdo proibido por lei.

5.4.**O Colaborador é responsável** por garantir a segurança, fidedignidade e adequação dos ficheiros que recebe e obtém através da Internet e Correio eletrónico. Todos os ficheiros que cheguem ao Colaborador a partir de origem externa à Organização devem ser sempre considerados suspeitos à partida, obrigando ao bom senso na confirmação de que proveem de fonte fidedigna e confiável.

5.5. **É proibido** o acesso a proxies remotos e a comunicações VPN de rede privada com mecanismos tunneling que permitam esconder e anonimizar os acessos ou ludibriar sistemas de auditoria e proteção das redes de comunicação. São exceção a esta regra os acessos a sites da função pública, ou acessos VPN fornecidos pela Organização.

5.6. **É proibida** a instalação de qualquer equipamento ou software na infraestrutura de comunicações ou computadores alterando, contornando ou colocando em risco as comunicações controladas pelo Serviço TI.

5.7. **É proibido** o acesso à Internet através de uma ligação alternativa aos acessos oficiais de comunicação disponibilizados pela Organização, nas instalações da Organização.

5.8. Em **caso de extinção do vínculo** com a Organização, o Colaborador deve eliminar do sistema a informação pessoal que não diga respeito à Organização.

5.9. O endereço de email institucional **não deve** ser utilizado com fins particulares para registo em plataformas de compras online, redes sociais, ou outras plataformas que não estejam relacionadas com as funções desempenhadas pelo colaborador.

6. Regras sobre UTILIZAÇÃO RESPONSÁVEL DAS CONTAS DE UTILIZADOR E PALAVRAS-PASSE

O Colaborador:

6.1. **NÃO PODE** autenticar-se nos sistemas com qualquer conta de utilizador que não lhe tenha sido atribuída;

6.2. **NÃO PODE permitir ou facilitar a terceiros o acesso** aos sistemas digitais da organização.

6.3. **NÃO revelar ou partilhar qualquer palavras-passe**, de nenhuma forma, seja com pessoas externas ou internas à Organização;

6.4. **NÃO DEVE deixar as suas palavras-passe gravadas num browser** internet de um equipamento que não seja do seu uso exclusivo;

6.5. **NÃO DEVE escrever as palavras-passe**, seja em papel ou em formato digital.

6.6. **DEVE manter confidencial qualquer palavras-passe de conta de grupo** de trabalho e não a pode revelar a pessoas que não pertençam a esse grupo de trabalho;

6.7. **DEVE evitar a visualização da digitação da palavra passe por terceiros**. A introdução deve ser efetuada no formato ilegível (ex. ****).

6.8. **DEVE manter confidencial qualquer palavras-passe** que utilize para aceder aos Sistemas Digitais da Organização ou qualquer outra que venha a ter conhecimento;

6.9. **DEVE alterar a palavra-passe** sempre que perceba que esta pode estar comprometida;

6.10. **DEVE alterar as palavras-passe em intervalos regulares no prazo máximo de 180 dias**. Mesmo quando tal não é exigido pelo sistema. As palavras-passe de contas privilegiadas devem ser alteradas mais frequentemente;

6.11. **DEVE bloquear ou terminar a sessão** sempre que não esteja junto do equipamento informático;

6.12. **DEVE manter seguros** todos os equipamentos informáticos com o pedido automático de palavra-passe por inatividade, fixada no máximo em 15 minutos.

7. Regras sobre CRIAR PALAVRAS-PASSE SEGURAS

O Colaborador está obrigado a criar Palavras-passe Seguras, respeitando as seguintes regras:

7.1. **Escolher palavras-passe fortes** que cumpram as regras de complexidade definidas pela Divisão de Informática e que não possam ser facilmente descobertas (De acordo com Resolução do Conselho de Ministros n.º 41/2018):

- Deve ter, no mínimo, 9 carateres;
- Tem de conter pelo menos um carater de 3 dos 4 conjuntos:
  - Letras minúsculas (a…z);
  - Letras maiúsculas (A…Z);
  - Números (0…9) ;
  - Carateres especiais (~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } [ ] : " ; ' < > ? , . /).
- NÃO PODE ser igual às 2 últimas anteriores;
- NÃO PODE ser derivada do nome identificador do utilizador;
- NÃO DEVE conter nomes de família;
- NÃO DEVE conter data de nascimento;
- Em alternativa poderá ser constituída por frase ou excerto de texto longo conhecido pelo utilizador, sem caracteres «espaço».

7.2. **DEVE EVITAR utilizar a mesma palavra-passe** para vários sistemas, especialmente aqueles mais críticos que podem por em maior risco a Segurança e Privacidade da Informação;

7.3. **NÃO DEVE utilizar as mesmas palavras-passe** para uso pessoal e profissional;

7.4. **Evitar reutilizar palavras-passe previamente usadas**;

8. Regras sobre ACESSOS REMOTOS

8.1 **O acesso remoto a um computador** de um utilizador por um colaborador ou pessoa não pertencente à Divisão de Informática, só pode ser efetuado após o consentimento da Divisão de Informática devidamente autorizado pelo Presidente.

9. Regras sobre CONSULTA OBRIGATÓRIA À DIVISÃO DE INFORMÁTICA

9.1 **O Colaborador não está autorizado** a instalar no computador qualquer software ou hardware;

9.2 **O Colaborador não está autorizado** a ligar qualquer equipamento digital externo às redes de comunicação internas da Organização;

9.3 A Divisão de Informática deve sempre ser Consultada para Avaliar tecnicamente a aquisição, alteração da atribuição e guarda de um recurso digital;

9.4 A Divisão de Informática deve ser Consultada para avaliação técnica antes de ocorrer a mobilidade do posto de trabalho do Colaborador e do equipamento que lhe está associado.

10. Regras sobre PROCEDIMENTOS EFETUADOS PELA DIVISÃO DE INFORMÁTICA

10.1 A Divisão de Informática pode auditar todos os sistemas digitais e redes de comunicação da Organização para garantir as melhores práticas de segurança e gestão dos sistemas digitais;

10.2 A Divisão de Informática pedirá ao Colaborador que remova das redes de comunicação internas da Organização, qualquer equipamento digital, informação ou software não autorizado por esta;

10.3 A instalação e configuração de Software nos equipamentos digitais da Organização apenas pode ser efetuada pela Divisão de Informática ou com a sua autorização;

10.4 A extinção do vínculo com a Organização determina o cancelamento e eliminação do conteúdo das contas de correio eletrónico após um período de 30 dias ou outro prazo acordado com o superior hierárquico do Colaborador.