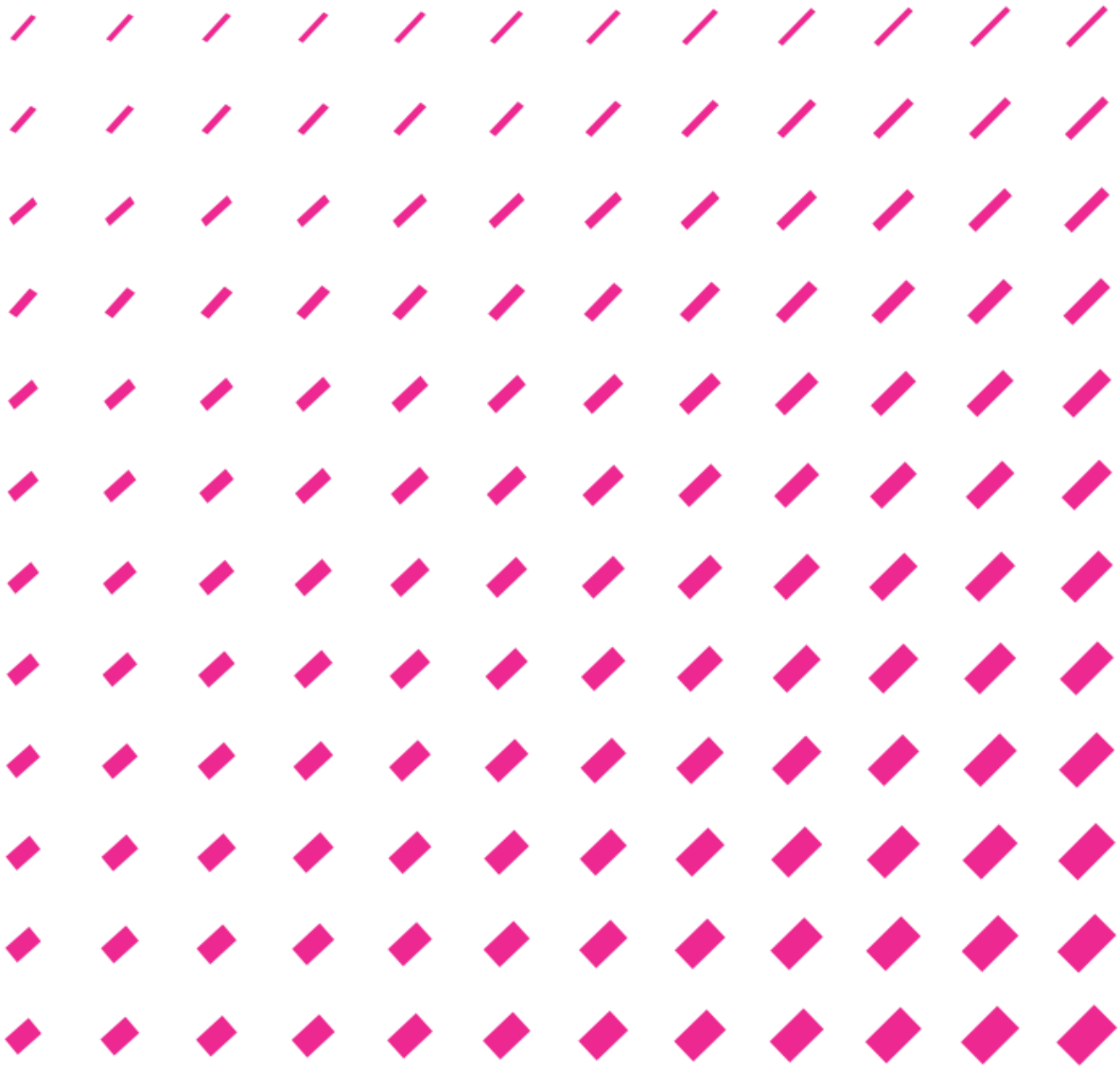
Bravantic

// Evolving Technology

Política da Segurança da Informação

V3.1



Quality & Certification

Aprovado por: Executive Committee

Bravantic®

// Evolving Technology

Índice

Controlo de Versão

Data	Versão	Criado por	Descrição da alteração
12/09/2019	1.0	João Moura	Versão Inicial
04/04/2023	2.0	João Ferreira	Revisão e formatação
22/02/2024	3.0	João Ferreira	Revisão e agregação com outras políticas do mesmo âmbito.
06/01/2025	3.1	João Ferreira	Adaptações ao alargamento de âmbito.

1 Objetivo

Esta política tem por objetivo a definição de linhas mestras, com vista à proteção dos ativos de informação da Bravantic, dos seus clientes, dos seus fornecedores e das restantes partes interessadas.

A implementação desta política está alinhada com as normas estabelecidas no Regulamento Interno da SI e demonstra o nosso compromisso com a Segurança da Informação, nas vertentes: Confidencialidade, Integridade e Disponibilidade.

2 Aplicabilidade

Esta política aplica-se a todos os colaboradores, subcontratados e fornecedores da Bravantic, no âmbito vigente do SGSI.

3 Política da Segurança da Informação

3.1 Aspetos gerais

É política da Bravantic:

i. Proteger a informação de acessos não autorizados;
ii. Manter a confidencialidade da informação;
iii. Assegurar que a informação não é divulgada a pessoas não autorizadas por meio de ação deliberada ou descuidada;
iv. Proteger a integridade da informação contra modificações não autorizadas;
v. Para a instalação de aplicações em sistemas em exploração, ter em conta as boias práticas recomendadas pela indústria, nomeadamente (entre outras): Tetes, rollback, documentação, formação, etc.
vi. Garantir a disponibilidade da informação para utilizadores autorizados, quando necessário;
vii. Atender aos requisitos regulamentares e legislativos;
viii. Documentar, manter e testar um Plano de Continuidade de Negócios;
ix. Formação e sensibilizar todos os colaboradores em aspetos relacionados com a Segurança da Informação.
x. Certificar-se de que todas as violações da Segurança das Informação são relatadas e investigadas.
xi. Velar pela melhoria contínua de processos, infraestruturas e conhecimento, relacionados com a Segurança da Informação.

3.2 Controlo de acessos

i. Apenas é facultado acesso físico às instalações e acesso lógico aos sistemas a colaboradores que tenham sido submetidos a entrevista de screening.
ii. Qualquer acesso facultado a colaboradores, subcontratados ou fornecedores da Bravantic será condicionado pelas funções que lhe forem atribuídas e revisto anualmente.
iii. O acesso de visitantes ao interior da Bravantic é apenas permitido quando estes estiverem acompanhados por um colaborador ou devidamente autorizados.
iv. A Bravantic mantém uma rede segregada para serviço dos visitantes, permitindo-lhes o acesso por wifi á internet.
v. Todos os acessos, físicos ou lógicos, são monitorizados e registados em log.

3.3 Utilização do Posto de Trabalho

i. Os postos de trabalho devem ser usados apenas para fins profissionais.

ii. Não é permitida a instalação de software não autorizado.
iii. Os colaboradores são responsáveis pelo uso adequado dos postos de trabalho, nomeadamente pela sua conservação, proteção contra utilização indevida e/ou ataques cibernéticos.

3.4 Utilização de dispositivos móveis

i. A utilização de dispositivos externos de armazenamento de dados deve ser limitada ao estritamente indispensável. Quando não estão a ser utilizados, os dispositivos externos devem ser guardados em local seguro.
ii. É obrigatória a utilização de firewall do dispositivo sempre que se pretenda aceder á rede da Bravantic a partir do exterior.
iii. Os dispositivos devem ser mantidos atualizados no que refere a antivírus e patches de segurança.
iv. Os telemóveis estão sujeitos á obrigatoriedade de uso de password.

3.5 Teletrabalho

i. É responsabilidade da Bravantic, fornecer aos seus colaboradores em teletrabalho, dispositivos móveis seguros, protegidos por passwords e por outras medidas de segurança como antivírus, firewalls e atualizações de segurança regulares.
ii. A Bravantic disponibiliza aos colaboradores em teletrabalho, meios seguros para acesso à rede interna.
iii. O acesso a plataformas, nomeadamente para desenvolvimento de software, deve ser sempre de forma encriptada.
iv. Quando acedem às contas ou aplicações, os utilizadores poderão ter de fornecer uma verificação de identidade adicional, por via de um código recebido no telemóvel (Autenticação multifactor - MFA).

3.6 Transferência de dados

A transferência de dados de e para a Bravantic, rege-se por um conjunto de políticas, nomeadamente:

i. Garantir o conhecimento absoluto da identidade do interlocutor.
ii. Utilizar meios de envio aprovados superiormente.
iii. Não transportar dados sensíveis em dispositivos externos, sem que estejam encriptados e/ou protegidos por password.
iv. Inteirar-se de que não existem acordos de confidencialidade que limitem o envio da informação.
v. O fluxo de informação deve ser monitorizável.
vi. Todas as ligações devem estar protegidas por firewall.

No Regulamento Interno da SI da Bravantic estão definidas um conjunto de normas de utilização da infraestrutura informática no sentido de promover a utilização responsável dos ativos (postos de trabalho, redes, aplicações e comunicações) colocados ao serviço de todos os colaboradores e confiados à Bravantic pelos clientes/utilizadores dos serviços constantes do âmbito do SGSI, de forma a assegurar o cumprimento desta Política da SI.

4 Melhoria Contínua

Cabe aos gestores do sistema identificar, por meio de avaliação de risco apropriada, o valor dos ativos de informação, entendendo as suas vulnerabilidades e as ameaças que podem expô-los a riscos.

Gerir os riscos para um nível aceitável através do desenho, implementação e manutenção do Sistema formal de gestão de segurança da informação.

5 Responsabilidades

A Gestão de Topo da Bravantic aprova esta política.

O gestor do Sistema de Gestão da Segurança da Informação facilita a implementação desta política por meio dos padrões, regulamentos e procedimentos apropriados.

Todo o pessoal tem a responsabilidade de denunciar incidentes de segurança, bem como quaisquer aspetos passíveis de desencadear ações de melhoria.

Qualquer ato deliberado que comprometa a segurança das informações de propriedade da Bravantic ou dos seus clientes ou fornecedores estará sujeito a ações disciplinares e/ou legais, conforme apropriado.

6 Revisão

A política é revista em intervalos planeados ou quando ocorrem alterações significativas de modo a assegurar a sua contínua aplicabilidade, adequabilidade e eficácia.