Política de Segurança Cibernética

PAMCARD

INFORMAÇÕES DO DOCUMENTO

Versão	Data	Status	Elaboração	Revisão	Aprovação	Modificações
1	02/2023	Concluído	Compliance	Segurança Cibernética DPO	Diretoria	Versão inicial

TERMOS E ABREVIAÇÕES

Termos	Definições
Aplicativo	Aplicações para celulares dispositivos de microinformática.
Colaboradores	Acionistas, administradores e empregados das empresas da Roadcard.
Confidencialidade	Garantia de que a informação somente possa ser acessada por pessoas autorizadas e pelo período necessário.
Dados Pessoais	Informações pessoais que podem ser associadas a uma pessoa identificada ou identificável. Dados Pessoais podem ser identificados como: nome, endereço (incluindo endereços de cobrança e entrega), número de telefone, e-mail, número do cartão de pagamento, outras informações financeiras, número da conta, data de nascimento e credenciais emitidas pelo governo (por exemplo, número da carteira de motorista, RG, passaporte, CPF e CNPJ).
Disponibilidade	Garantia de informação disponível para as pessoas autorizadas quando se fizer necessária.
Incidente	Resultado de uma ameaça que explora uma ou mais vulnerabilidades, levando à perda dos requisitos da confidencialidade, integridade e disponibilidade da informação.

Informações Protegidas	Todo e qualquer dado ou informação que o Colaborador ou Prestador de Serviços desenvolva ou venha a ter acesso, direta ou indiretamente, em qualquer formato (oral ou escrito, seja em suporte físico ou digital), em virtude do seu vínculo com a Roadcard ou do desempenho de suas atividades contratadas pela Roadcard, incluindo dados pessoais e não-pessoais.
Integridade	Garantia de informação completa, exata, íntegra e não modificada ou destruída indevidamente, de maneira não autorizada ou acidental durante o seu ciclo de vida.
Monitoramento	Prerrogativa da Roadcard de controlar, acessar, vistoriar e fiscalizar com a finalidade de acompanhar se todo seu ambiente físico e digital cumpre as diretrizes desta Política de Segurança Cibernética, bem como observa os demais requisitos legais.
Prestadores de serviços	Qualquer pessoa física ou jurídica que preste serviços para as empresas da Roadcard ou que estabeleçam relação comercial de parceria.
Site	Quaisquer produtos, serviços, conteúdo, recursos, tecnologias, funções, todos os sites, aplicativos e serviços relacionados oferecidos ao Usuário pelo A Roadcard em conexão a uma Conta ou Transação de Convidado.
Usuário	Indivíduo que utiliza os Serviços ou acessa o Site e tenha estabelecido um relacionamento com a Roadcard (por exemplo, ao abrir uma Conta e concordar com os Termos & Condições da Roadcard) ou de outra forma usa os Serviços como comprador, vendedor ou outro tipo de participante de uma transação, incluindo o Visitante.

1. Introdução

A Roadcard se preocupa com a segurança dos Dados Pessoais e Financeiros de seus Usuários, Colaboradores e Prestadores de Serviços, e de suas próprias informações, por isso é comprometida com a proteção de todos esses dados.

Para isso, a Roadcard utiliza as mais avançadas tecnologias de proteção de dados existentes no mercado e seleciona criteriosamente os Colaboradores e Prestadores de Serviços para prestação de serviços de processamento, armazenamento de dados e de computação em nuvem.

A Política de Segurança Cibernética foi desenvolvida para dar diretrizes sobre os padrões de segurança esperados e para coordenar os procedimentos e controles das informações da Roadcard, sejam elas físicas ou eletrônicas.

2. Objetivo

Este documento tem por objetivo estabelecer as diretrizes para o funcionamento da Política de Segurança da Informação na Roadcard, orientando seu quadro funcional, seus colaboradores e parceiros para a busca da melhoria contínua das atividades relacionadas ao planejamento, execução, análise dos seus processos/produtos e proteção das informações geradas e tratadas no âmbito da empresa.

A informação como ativo de valor para a Roadcard requer tratamento adequado e, para tal, faz-se necessário a adoção de diretrizes que permitam as ações. Com a participação não somente das áreas de negócio, mas também de todos os colaboradores que, direta ou indiretamente, estão ligados aos negócios da empresa, a gestão desse ativo deve ser eficiente e eficaz buscando minimizar quaisquer riscos inerentes ao negócio.
A presente Política de Segurança da Informação, dessa maneira, tem por intuito sistematizar as diretrizes voltadas a proteger tais elementos nos mais diversos âmbitos da atuação profissional na Roadcard. Além disso, a Política de Segurança Cibernética lista os procedimentos e controles internos para prevenir, detectar e reduzir a vulnerabilidade à ocorrência de incidentes cibernéticos. A Roadcard se compromete, por meio desta Política, a oferecer recursos necessários à melhoria contínua dos procedimentos aqui dispostos e relacionados à segurança cibernética.

3. Base Legal

A base normativa inclui, mas não se limita aos seguintes diplomas:

Resolução BCB nº 85/2021
Lei Geral de Proteção de Dados nº 13.708/2018
Marco Civil da Internet nº 12.965/2014
Decreto nº 8.771/2016
ISO/IEC 27001:2013

4. Propriedade Intelectual das Informações

4.1 A Confidencialidade é uma premissa importante para os negócios da Roadcard. Todo e qualquer dado ou informação que o Colaborador ou Prestador de Serviço desenvolva ou venha a ter acesso, direta ou indiretamente, em qualquer formato (oral ou escrito, seja em suporte físico ou digital), em virtude do seu vínculo com a Roadcard ou do desempenho de suas atividades contratadas pela Roadcard (as "Informações Protegidas"), será considerada informação confidencial, de exclusiva propriedade da Roadcard, sendo expressamente proibida a sua reprodução, divulgação, publicação, transmissão, cessão ou facilitação de seu acesso a quaisquer terceiros, direta ou indiretamente, total ou parcialmente, salvo se autorizado por escrito, de maneira prévia e expressa, pelos representantes da Roadcard.

4.2 O Colaborador ou Prestador de Serviços será o único e exclusivo responsável pelo uso que fizer das Informações Protegidas. O eventual uso indevido, por negligência, imprudência, imperícia ou até mesmo intencional a que o Colaborador ou Prestador de Serviços fizer das Informações Protegidas será de sua exclusiva responsabilidade, isentando a Roadcard de toda e qualquer responsabilidade nesse sentido. A Roadcard reserva-se o direito de monitorar o uso das Informações Protegidas pelo Colaborador ou Prestador de Serviços e analisar todos dados e evidências relacionados, para fins de obtenção de provas que poderão ser eventualmente utilizados nos processos investigatórios e na adoção das medidas legais cabíveis. Em caso de desvio das regras assim determinadas o colaborador ou Prestador de Serviços poderá sofrer as penalidades previstas nesta Política, sem prejuízo das demais penalidades impostas no Código de Conduta da Roadcard.

4.3 A qualquer tempo, caso seja solicitado pela Roadcard, ou em caso de finalização da relação do Colaborador ou Prestador de Serviços com a Roadcard, independentemente da causa, o Colaborador ou Prestador de Serviços restituirá a Roadcard todas as cópias, bancos de dados, reproduções e/ou adaptações que porventura tiver realizado das Informações Protegidas. O Colaborador ou Prestador de Serviços reconhece, ainda, que as obrigações e proibições previstas nesta cláusula permanecerão válidas durante toda a existência do vínculo do Colaborador ou Prestador de Serviços com a Roadcard, mesmo após o término de tal vínculo, independentemente do motivo.

4.4 Qualquer Informação Protegida cuja divulgação seja exigida por Lei, ordem judicial, determinação de autoridades administrativas competentes ou acordos celebrados pela Roadcard com terceiros, somente poderá ser divulgada por meio da área Jurídica da Roadcard.

5. Classificação das Informações Protegidas

5.1 Para assegurar a proteção adequada das Informações Protegidas a Roadcard classifica as informações internamente de acordo com a importância que representam. São consideradas informações confidenciais toda e qualquer informação, dado ou fato, por escrito, verbal ou de qualquer outro modo apresentado, relacionados à Roadcard, sejam bancos de dados, planilhas, dos sistemas integrados, ERP, CRM, RH, Pamcard, Pambank e IBM, além de atendimentos telefônicos, da sua gravação e monitoramento, bem como quaisquer outros que venham a ser implementados pela empresa, arquivos, figuras, mensagens, documentos eletrônicos recebidos ou enviados, através da internet ou e-mail.

6. Manuseio das Informações Protegidas

6.1 O Colaborador ou Prestador de Serviços é responsável pelo uso que fizer das Informações Protegidas. Assim, as regras de Segurança Cibernética deverão ser observadas abaixo para garantir um nível mínimo de segurança da informação.

6.2 Os colaboradores da Roadcard, bem como indivíduos que ocupem posições executivas, devem se comprometer a não utilizar ou divulgar os dados e informações a que têm acesso, a não ser para atender ao fim restrito para o qual os dados foram confidenciados, mediante autorização expressa do Encarregado de proteção de dados.

6.2.1 Os colaboradores receberão e deverão assinar termo de compromisso em que tomam ciência de seus deveres de confidencialidade.

6.3 Os membros e colaboradores da Roadcard não devem acessar, ou tentar ter acesso, aos dados confidenciais que não são necessários para a execução de suas tarefas ou que exorbitem da finalidade de sua atuação ou cargo.

6.4 O dever de proteção à confidencialidade, que compreende tanto o sigilo profissional, quanto o cuidado com a proteção das informações confidenciais internas da Roadcard, deve ser observado em todas as atividades desempenhadas em decorrência do vínculo com a empresa.

6.5 Os profissionais não devem discutir informações confidenciais em locais públicos como corredores, elevadores, restaurantes e transportes públicos

6.6 Também no ambiente físico os integrantes da Roadcard devem adotar condutas de armazenamento seguro e adequado de informações confidenciais e sensíveis.

6.7 Informações confidenciais ou sensíveis não deverão ficar expostas em locais como mesas, armários e/ou quaisquer móveis localizados no âmbito da empresa fora do momento de sua utilização.

6.8 Após sua utilização, todo o material com informações confidenciais ou sensíveis deverá ser armazenado de maneira segura em gavetas, armários e/ou outros meios protegidos por chaves, ou outros mecanismos que ofereçam a segurança necessária ao acesso.

6.9 Os integrantes da Roadcard devem adotar as cautelas necessárias à ocultação de informações ou bloqueio de suas telas, preferencialmente com senha, ao se ausentarem de suas estações de trabalho.

Deveres e Cautelas relacionados a proteção e integridade das informações

6.10 A preservação da integridade das informações é requisito essencial à própria continuidade das atividades da Roadcard, de sorte que quaisquer riscos que possam afetar a integridade das informações devem ser prioritária e urgentemente endereçados, afastados e/ou mitigados.

6.11 Todas as atividades da Roadcard devem ser constantemente submetidas a análises e varreduras antivírus, anti-malware e anti-spyware, bem como devem estar protegidas por firewall.

6.12 As mídias removíveis utilizadas pelos integrantes da Roadcard devem ser previamente validadas pelo Departamento de Tecnologia da Informação.

6.13 As mídias removíveis utilizadas pelos integrantes da Roadcard devem passar por varredura antivírus antes de serem utilizadas.

6.14 Qualquer incidente que afete a integridade de dados deve ser imediatamente notificado ao Encarregado de proteção de dados e ao Departamento de Tecnologia da Informação.

6.15 Qualquer incidente que afete a integridade de dados deve ser seguido de auditoria, a ser conduzida pelo Encarregado de proteção de dados, voltada a:

I – Garantir a continuidade da prestação de serviços pela Roadcard;
II – Recuperar e/ou reorganizar os dados afetados pelo incidente;
III – Identificar eventuais indivíduos afetados pelo incidente;
IV – Mapear responsabilidades e procedimentos a serem instaurados após o incidente.

7. Perfil, Identificação, Credenciais de Acesso e Equipamentos

7.1 Todos os Colaboradores ou Prestadores de Serviços possuem perfis de acesso às Informações Protegidas, definidos pela Roadcard, de acordo com seu cargo e atribuições.

7.2 A Roadcard possui procedimentos de controle destinados a identificar as pessoas autorizadas a acessarem os dados e documentos de cada processo, especialmente os sigilosos.

7.3 A forma ou nível de acesso aos documentos guardados por sigilo não precisa ser igual e/ou uniforme para todos aqueles autorizados a conhecerem o seu conteúdo, sendo indicada a definição de permissões especiais para o manuseio, a retirada de cópias, a alteração das condições de guarda ou acesso, inclusive a pastas, dentre outros elementos.

7.4 A Roadcard reserva-se o direito de revisar, a qualquer momento e sem aviso prévio, os privilégios de qualquer Colaborador ou Prestador de Serviços, a fim de resguardar os níveis de segurança da informação da Roadcard.

7.5 Os equipamentos fixos ou móveis de computação ou comunicação a serem utilizados pelos colaboradores e membros da Roadcard são previamente validados pelo Departamento de Tecnologia da Informação antes de sua aquisição e/ou de sua implementação nas atividades profissionais.

7.6 Na hipótese de trabalho remoto, os dispositivos são novamente submetidos ao crivo do Departamento de Tecnologia da Informação para análise adicional quanto à idoneidade e segurança do hardware e do software a serem utilizados.

7.7 Equipamentos e instalações voltadas ao processamento de informação crítica ou sensível, ou que sirvam para a manutenção de infraestruturas centrais de armazenamento e/ou de rede, são mantidos em áreas seguras, com as devidas salvaguardas contra ameaças físicas e ambientais e controles de acesso.

7.8 Todos os recursos de computação e comunicação móvel são, no momento de sua substituição e/ou troca, devolvidos à área responsável, juntamente com seus periféricos conforme procedimento específico.

7.9 A tomada de decisão a respeito dos equipamentos e serviços a serem adquiridos ou contratados pela Roadcard envolve, para além do responsável de área, o Encarregado de proteção de dados e o Departamento de Tecnologia da Informação.

7.10 O acesso aos recursos de computação, correio eletrônico, envio de mensagens e outros meios de comunicação ocorre através das interfaces disponibilizadas com a utilização de conta de usuário, POR

intermédio de autenticação e autorização, os quais são considerados dados confidenciais e intransferíveis. O usuário poderá configurar filtros de mensagens fazendo uso de interface específica. Tais filtros serão de responsabilidade exclusiva do usuário.

7.10.1 O usuário deverá utilizar respostas automáticas em hipóteses de ausência, sempre indicando os dados de contato do sujeito responsável por suas funções no período em questão.

7.11 A utilização dos recursos de computação e comunicação disponibilizados pela Roadcard é restrita às atividades profissionais vinculadas à própria empresa.

7.12 É obrigatória a inclusão, nas mensagens eletrônicas, do texto abaixo objetivando classificar as informações contidas nas mensagens e o tratamento a ser dado em casos de erros de envio:

"As informações contidas nesta mensagem, incluindo seus anexos, são CONFIDENCIAIS e protegidas pelo sigilo legal. Caso não seja o destinatário, favor apagá-la e notificar seu remetente imediatamente. A leitura, divulgação ou cópia são proibidas e estará sujeita às normas da empresa e/ou a legislação em vigor"

7.13 É vedada a utilização de servidores de e-mail gratuitos para envio de informações ou documentos atinentes às atividades da Roadcard, sendo obrigatória a utilização do e-mail institucional e a utilização de dispositivos públicos ou pessoais não autorizados para o acesso a documentos atinentes às atividades da Roadcard. A utilização de um recurso pessoal para acesso remoto a outro recurso da Roadcard só será permitida exclusivamente com a utilização da VPN estabelecida pela própria empresa, seguindo os parâmetros de autenticação e autorização determinados pela área de Segurança da Informação.

7.14 Não será autorizada a utilização dos recursos de comunicação da Roadcard para o tráfego de mensagens eletrônicas contendo:

I - Material obsceno, ilegal, ofensivo ou não ético;
II - Listas de endereços eletrônicos dos colaboradores da empresa;
III - Vírus ou qualquer código malicioso;
IV - Material protegido por propriedade intelectual;
V - Entretenimentos e correntes;
VI - Material preconceituoso ou discriminatório;
VII - Material de natureza político-partidária ou sindical, que promova a eleição de candidatos para cargos públicos eletivos, clubes, associações e sindicatos;
VIII - Arquivos de músicas, vídeos ou animações que não sejam de interesse da empresa;
IX - Mensagens de despedida;

X - Mensagens consideradas SPAM;
XI - Dados pessoais de quaisquer origens sem o devido fim profissional e de necessidade do negócio da empresa.

8. Senhas e deveres de cautela relacionadas ao uso de serviços de informática e em rede

8.1 As senhas de acesso aos dispositivos e servidores da Roadcard permitem identificar o Colaborador ou Prestador de Serviços como o responsável pelas atividades que praticar usando a infraestrutura da Roadcard. Por esse motivo, cada Colaborador ou Prestador de Serviços é exclusivamente responsável por todas as suas senhas de acessos, que são pessoais, intransferíveis e de uso exclusivo do Colaborador ou Prestador de Serviços.

8.2. As senhas a serem utilizadas para acesso aos sistemas e dispositivos da Roadcard devem ser criadas de forma a possibilitar a maior proteção possível, devendo ter pelo menos 08 (oito) caracteres, necessariamente contendo letras maiúsculas, minúsculas, numerais e caracteres especiais, e não devendo conter nomes associados ao seu titular, datas de nascimento, dentre outras informações pessoais de fácil inferência, além disso não é possível fazer a reutilização das últimas 03 senhas.

8.3 Ao se ausentar do local de trabalho, o profissional deverá bloquear seu computador, com vistas a evitar que outras pessoas o utilizem, sendo vedada a opção por salvar senhas de acesso.

8.4 É vedado o compartilhamento de senhas de acesso aos sistemas internos da Roadcard ou de terceiros, de tokens ou de outras formas de acesso, bem como de senha de acesso ao e-mail institucional, tanto com colegas de trabalho, quanto com terceiros, salvo em situações de excepcional relevância ou urgência que tenham sido devidamente autorizadas pelo Encarregado de proteção de dados.

8.5 É vedada a utilização de redes públicas para o envio ou recebimento de informações atinentes às atividades da Roadcard, incluindo, mas não se limitando, a redes de cafés, restaurantes, centros comerciais e aeroportos;

8.6 A realização de serviços em home office, se autorizada pela administração, deve observar padrões ainda mais rígidos de segurança, especialmente quanto à privacidade de rede e ao acesso remoto a arquivos da Roadcard, devendo-se:

I – Evitar o compartilhamento de dados profissionais para e-mail pessoal sem a prévia autorização da administração;
II – Utilizar de acesso remoto (VPN) autorizado pela empresa;
III – Utilizar de redes privadas, evitando-se ao máximo o uso de redes públicas;
IV – Utilizar preferencial de dados de login da empresa em websites com certificação de segurança (chaves criptográficas, prefixo HTTPS, dentre outros);
V – Utilizar de equipamentos e mídias removíveis homologados e aprovados pela empresa e sua equipe de tecnologia;
VI – Utilizar a configuração de logins e senhas de redes residenciais para padrões seguros;
VII – Realização semanal de backups;
VIII –Realizar testes de segurança via dupla autenticação, antivírus, dentre outros mecanismos aprovados pela equipe de tecnologia da empresa.

8.7 A utilização de sistemas de mensagens instantâneas para envio de informações e arquivos relacionados às atividades da Roadcard somente é permitida se ativada a opção de criptografia de ponta a ponta.

8.8 Deve-se, quando possível, priorizar a utilização de serviços off-line para análise e manipulação de documentos, como para a combinação, divisão ou compressão de arquivos.

9. Procedimentos e Controles

9.1 Autenticação

Os sistemas e equipamentos da Roadcard possuem controle de acesso pessoal, único e intransferível, de modo a assegurar o seu uso apenas por usuário autorizado, seja Colaborador ou Prestador de Serviço.

9.2 Criptografia

9.2.1 As informações classificadas como Confidenciais, Restritivas ou Secretas devem ser protegidas contra acesso não autorizado.

9.3 Prevenção e Detecção de Intrusão

A Roadcard possui mecanismos para prevenção e detecção de falhas de segurança. Possuímos segurança de borda através dos nossos firewalls e rígido controle de autenticação de duplo fator para

acessos remotos. Nossas aplicações são protegidas por firewalls específicos para tais funções (WAF – Firewall para aplicações Web) e possuímos ainda tecnologia que varrem periodicamente todo o nosso ambiente para identificação e tratamento de novas vulnerabilidades sejam elas de aplicações Web ou de infra-estrutura.

9.4 Prevenção de Vazamento de Informações

A Roadcard adota medidas para prevenir o vazamento de informações, tanto pelos Colaboradores ou Prestadores de Serviços, quanto por invasões externas. Possuímos ferramentas de DLP e CASB que nos auxiliam na prevenção do vazamento de informações tanto no ambiente on premisses quanto no ambiente cloud.

9.5 Mecanismo de Rastreabilidade

A Roadcard possui mecanismos para rastreabilidade dos acessos aos seus Site, Aplicativo, plataformas e rede. Possuímos ferramenta de SIEM que nos permite correlacionar os logs gerados em nossos ambientes para uma ágil interpretação dos acontecimentos e tomada de decisão.

10. Treinamento

A Roadcard promove a capacitação por meio de treinamentos, boletins e informativos, reciclagem e o aperfeiçoamento de todos seus Colaboradores para garantir a segurança das Informações Protegidas e a execução das atividades respeitando as melhores práticas de Segurança Cibernética.

11. Terceirização de serviços de processamento, armazenamento de dados e de computação em nuvem

Os contratos com a Roadcard e as prestadoras de serviços que possuem acesso às informações, aos sistemas e/ou ao ambiente da Roadcard contêm cláusulas que dispõem sobre o cumprimento dessa Política Cibernética, legislação e normas do Banco Central aplicáveis e penalidades em caso de descumprimentos.

12. Desenvolvimento Seguro

Todos os colaboradores ou Prestador de Serviços, integrantes das equipes técnicas de engenharia responsáveis pelo desenvolvimento da Roadcard, possuem diretrizes de desenvolvimento seguro.

13. Segregação de Ambientes

13.1 Os integrantes da Roadcard devem, sob a supervisão do Encarregado de proteção de dados e o apoio do Departamento de Tecnologia da Informação, zelar pela adequada segregação dos ambientes de produção, homologação, desenvolvimento e demais ambientes necessários paras as aplicações e sistemas da empresa.

13.2 Os ambientes de desenvolvimento, homologação ou qualquer outro que não seja o de produção, devem ser segregados de maneira lógica e o ambiente de produção deve ser segregado de maneira física e lógica dos demais ambientes da Roadcard.

13.3 O formato dos dados que serão usados nos ambientes poderá ser o mesmo, mas em hipótese alguma dados do ambiente de produção poderão ser usados em outros ambientes.

14. Monitoramento e Auditoria

A Roadcard deve monitorar e registrar todo o uso das informações geradas, armazenadas ou veiculadas na empresa. Para tanto, a Roadcard deve manter controles apropriados e trilhas de auditorias ou registros de atividades em todos os pontos e sistemas que a empresa julgar necessário para reduzir os riscos, e reservar-se o direito de:

- Implantar sistemas de monitoramento de acesso às estações de trabalho, servidores internos e externos, correio eletrônico, navegação, Internet, dispositivos móveis ou *wireless* e outros componentes da rede. A informação gerada por estes sistemas de monitoramento poderá ser usada para identificar usuários e respectivos acessos efetuados;
- Inspecionar qualquer arquivo que esteja na rede, no disco local da estação ou qualquer outro ambiente, visando assegurar o rígido cumprimento desta PSI; e

- Instalar sistemas de proteção e detecção de invasão para garantir a segurança das informações e dos perímetros de acesso.

15. Das responsabilidades Específicas

15.1 Dos colaboradores em geral

Os colaboradores e prestadores de serviços da Roadcard, em qualquer nível hierárquico, na sua esfera de competência, serão responsáveis em cumprir, fazer cumprir e zelar pela materialização e realização eficaz das normas e dos princípios da segurança da informação, no compromisso com os critérios legais e éticos que envolvem a Companhia.

É de inteira responsabilidade de cada colaborador e/ou prestador de serviço qualquer prejuízo ou dano que vierem a sofrer ou causarem a empresa e/ou terceiros, em decorrência do não atendimento às diretrizes dessa Política e das Normas aqui referidas.
É de responsabilidade do colaborador e/ou prestador de serviço o uso de senha segura, devendo altera-la conforme periodicidade já descrita na presente política.

Cabe a todos os colaboradores e/ou prestador da Roadcard:

- Cumprir fielmente Políticas e Normas de Segurança da Informação estabelecidas neste ou em qualquer outro documento publicado pela área de Segurança da Informação;
- Buscar a orientação do superior hierárquico, quando houver dúvidas relacionadas à segurança da informação;
- Proteger as informações contra o acesso, modificação, divulgação ou destruição não autorizada pela Roadcard;
- Assegurar que os recursos tecnológicos sejam utilizados somente para fins profissionais aprovados e de interesse da Roadcard;
- Comunicar a área de Segurança da Informação sobre qualquer descumprimento ou violação desta Política e/ou de suas normas relacionadas;

15.2 Da área de Segurança da Informação

Cabe ao time de Segurança da Informação:
Prezar pelo cumprimento dos itens definidos nesta política;
Promover ações de conscientização em Segurança da Informação;
Realizar atualização anual desta Política e documentos pertinentes a Segurança da Informação de acordo com as normas e melhores práticas, e;
Realizar em conjunto com Compliance, treinamentos e desenvolver materiais para disseminação do conhecimento;

15.3 Dos Gestores

É responsabilidade de cada gestor inventariar, atribuir valor, analisar quanto aos riscos e classificar, junto com as áreas de Compliance e de Controles Internos todos os ativos de informação necessária à sua área.
Garantir na sua área implementação de mecanismos necessários para descarte seguro das informações.
Cabe a todo gestor da área:

- Ter postura exemplar em relação à Segurança da Informação, servindo como modelo de conduta para os colaboradores internos sob a sua gestão;
- Cumprir e fazer cumprir essa Política e Normas de Segurança da Informação;
- Assegurar que suas equipes possuam acesso e conheçam essa política, bem como as normas aqui estabelecidas;
- Atribuir na fase de contratação de terceirizados e parceiros, quando este necessita ter contato com informações da companhia a inserção de cláusula de responsabilidade, ciência da norma de segurança da Informação para fornecedores e confidencialidade, exigindo o repasse das obrigações a seus colaboradores responsáveis pela prestação de serviços dentro da Companhia; e,
- Especificar e solicitar previamente permissão de acesso, elencando os ativos de informação para prestadores de serviços em geral que não sejam contratados.

15.4 Da área de Tecnologia da Informação
A área de TI será responsável:

- Pela gestão do uso de tecnologias necessárias ao bom andamento dos negócios da Roadcard, incluindo ações preventivas e tratamento de incidentes a fim de promover maior nível de segurança de informação;
- Em propor as metodologias e processos específicos para a Segurança da Informação como por exemplo, Avaliação de Risco;
- Em propor e apoiar iniciativas que visem à segurança dos ativos de informação da Roadcard;
- Em apoiar a avaliação e a adequação de controles específicos de Segurança da Informação para novos sistemas ou serviços; e
- Em manter comunicação efetiva com o Comitê de Segurança da Informação, com o objetivo de mantê-los adequadamente informados sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a Roadcard.

15.5 Do Compliance
Cabe a área de Compliance:

- Acompanhar incidentes que violem significativamente a Política de Segurança da Informação e as Normas de Segurança da informação;
- Acompanhar o processo disciplinar, validando as penalidades e exceções, quando houver;
- Revisar periodicamente e sugerir adaptação desta Política e Normas de Segurança da Informação de acordo com as necessidades e perfil de incidentes ao longo do tempo; e
- Acompanhar os normativos e legislação aplicáveis à Segurança da informação e, com base nelas, auxiliar a área de Tecnologia da Informação na revisão dos documentos internos da Roadcard que tratem sobre o tema.

10.6 Do Recursos Humanos

Cabe à área de Recursos Humanos atribuir, na fase de contratação dos colaboradores e formalizar nos contratos individuais de trabalho, a responsabilidade quanto ao cumprimento da Política de Segurança da Informação dos colaboradores já contratados, bem como efetuar o arquivamento da mesma; e

- Comunicar a área de Segurança da Informação/TI formal e prontamente toda e qualquer alteração no quadro funcional da Roadcard, contratações, demissões, alterações de cargos, funções, entre outros necessários, em prazo mínimo, a fim de evitar acessos não autorizados e/ou desnecessários.

16. Exceções

Eventuais casos especiais devem ser tratados e previamente autorizados pelo Departamento de Segurança da Informação.

15. Penalidades

O descumprimento dessa política e qualquer outro documento que a apoie poderá implicar em medidas administrativas e/ou jurídicas cabíveis, resguardando os interesses da Roadcard, podendo inclusive implicar em responsabilidade civil, responsabilidade criminal e resolução de contratos.