1. FINALIDADE

Estabelecer diretrizes para garantir a efetiva proteção dos dados, informações e conhecimentos gerados, bem como a redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confiabilidade, autenticidade das informações na CPTM e a continuidade dos seus negócios.

2. ABRANGÊNCIA

Aplica-se a todos os membros estatutários, diretores, empregados, estagiários, alunos aprendizes, além dos fornecedores, prestadores de serviços e parceiros, bem como toda pessoa física ou jurídica que, de alguma forma, executem atividades funcionais amparadas por contratos ou instrumentos jurídicos e que, para tanto, venham a utilizar ou ter acesso às informações de propriedade da CPTM ou sob sua custódia, em qualquer meio, especialmente, físico ou eletrônico.

3. DEFINIÇÕES

3.1. Acesso

Ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique.

3.2. Armazenamento

Consiste na guarda da informação, seja em um banco de dados, em papel, em mídia eletrônica, entre outros.

3.3. Armazenamento e Operações de Dados

Fornecem suporte durante todo o ciclo de vida dos dados para maximizar seu valor, desde o planejamento e design até o descarte dos dados.

3.4. Ativos de Informação

São ativos de tecnologia da informação, dados, documentos ou qualquer outro elemento que possua valor e esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível.

3.5. Ativos de Tecnologia da Informação

Quaisquer meios de armazenamento, transmissão e tratamento das informações, como softwares, hardwares e ambientes físicos.

3.6. Autenticidade

Garantia de que a informação é livre de adulteração.

3.7. Classificação da Informação

Atribuição, pela autoridade competente, da classificação do uso atribuído à informação.

3.8. Comitê de Crise de Segurança da Informação

Este comitê deve ser formado por equipe multidisciplinar de gerenciamento de crises e incidentes de segurança.

3.9. Confidencialidade

Propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, sistema, órgão público ou entidade não autorizados ou credenciados.

3.10. Dado Pessoal

Informação relacionada a pessoa natural identificada ou identificável.

3.11. Descarte

Eliminação correta de informações, documentos, mídias e acervos digitais.

3.12. Disponibilidade

Propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão público ou entidade devidamente autorizados.

3.13. Incidente de Segurança com Dados Pessoais

Qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do Titular de Dados Pessoais.

3.14. Incidente de Segurança da Informação

Qualquer evento adverso confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando à perda individual ou conjunta da confidencialidade, integridade e disponibilidade.

3.15. Informação

É o conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.

3.16. Integridade

Propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

3.17. Plano de Contingência de Segurança

É um documento formal da organização no qual estão descritos todos os protocolos de ações para os casos de concretizações de riscos de segurança. Visa garantir a pronta resposta da segurança para os casos ocorrências de eventos indesejáveis e danosos aos interesses da organização. Devendo promover:

- Comunicação de desvios e falhas de segurança;
- Mobilização do Comitê de Crise de Segurança;
- Registro dos incidentes e das evidências;
- Procedimentos para proteção das evidências de forma adequada;
- Análise forense computacional e;
- Ações de resposta ao incidente, com combate, controle e recuperação.

4. DIRETRIZES

4.1. Gerais

- As diretrizes desta Política estão apoiadas nos seguintes princípios:

Integridade – É vedada a manipulação das informações, portanto, são proibidas alterações, supressões e adições de conteúdo nas informações, salvo se expressamente autorizadas pela companhia.

Confidencialidade – Somente pessoas devidamente autorizadas pela CPTM devem ter acesso à informação.

Disponibilidade – A informação deve estar disponível para as pessoas autorizadas, sempre que necessário ou demandado.

Rastreabilidade – Possibilita acompanhar ou identificar o percurso deum dado ou informação durante um processo: saber onde, como, por quem e quando o dado foi manipulado, quando possível.

- Esta Política será amplamente divulgada interna e externamente visando a sua disponibilidade para todos que se relacionam com a CPTM e que, direta ou indiretamente, são impactados.

- O gerenciamento da segurança da informação na CPTM será disciplinado por meio de Normas, Procedimentos e Padrões específicos, respeitadas as diretrizes gerais contidas nesta Política e observado o estabelecido pela legislação reguladora da matéria.

- A Gerência de Tecnologia da Informação - GFI deverá elaborar um Plano de Contingência, para nortear os procedimentos a serem seguidos em situação de

crise. O Plano de Contingência deve ser atualizado regularmente para se manter atualizado com as melhores práticas de segurança e mudanças internas e externas.

- As ocorrências de violações a esta Política devem ser avaliadas pela área responsável pela informação juntamente com Gerência de Tecnologia da Informação - GFI, independentemente das instâncias de apuração de responsabilidades.

4.2. Proteção da Informação

- Todas as informações e sistemas de propriedade da CPTM ou sob sua custódia devem ser mantidos em locais protegidos.

- Deve ser mantido sigilo sobre toda e qualquer informação ou dado a que tiver acesso, não se valendo desse privilégio em benefício próprio ou de terceiros, mesmo depois de findo o vínculo contratual.

- Não é permitido manter acessíveis ou permitir acesso a pessoas não autorizadas, documentos e informações em qualquer tipo de mídia (eletrônica, impressa ou outros).

- Todos os dados armazenados em banco de dados em produção somente poderão ser reproduzidos com autorização formal.

- Todo tráfego de informações entre aplicação e banco de dados deve ser criptografado sempre que possível.

- Toda informação pertencente à CPTM ou sob sua custódia deverá possuir mecanismos de proteção e classificação.

- A classificação dos dados é sempre realizada pelo proprietário da informação, seja ele interno ou externo, levando-se em consideração o disposto na Lei Federal nº 12.527/2011 - Lei de Acesso à Informação (LAI) e Lei Federal nº 13.709/2018 - Lei Geral de Proteção aos Dados Pessoais (LGPD).

- No mesmo sentido, as informações pertencentes à CPTM ou sob sua custódia serão classificadas segundo grau de sigilo, a ser tratado em política própria.

- Toda informação de dados pessoais será tratada de acordo com os princípios legais aplicáveis, em especial a proteção da privacidade do titular dos dados, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento econômico e tecnológico.

- O acesso às bases de dados dos sistemas em produção deve ser realizado somente pelas aplicações de produção ou pelos técnicos (Database Administrator – DBA) responsáveis pela manutenção dos bancos de dados.

- Todo acesso físico às dependências da CPTM deverá ser previamente autorizado, controlado e monitorado.

- Para acessar os sistemas da CPTM, os usuários devem fazer uso de senhas/credenciais atribuídas para tal finalidade. Toda senha ou credencial de acesso é pessoal e intransferível e não deve ser divulgada e/ou compartilhada com terceiros.

4.3. Uso dos recursos de Tecnologia da Informação (TI)

- Os recursos (hardware e software) mantidos (em qualquer meio) pela CPTM é de sua propriedade e somente podem ser utilizados/manipulados por pessoas autorizadas e para uso corporativo.

- Todo uso será passível de monitoramento, sem aviso prévio, por parte da CPTM, por pessoal devidamente autorizado, sem se limitar ao acesso à internet, às mensagens recebidas e enviadas e arquivos mantidos sob qualquer forma.

- Na condução de monitoramento, a CPTM preservará, de acordo com a legislação vigente, a confidencialidade das informações e a privacidade dos envolvidos.

- É proibido o uso dos recursos de TI da CPTM para conduzir negócios estranhos às suas funções profissionais, realizar atividades para fins de ganhos pessoais, propaganda pessoal, angariar ou promover causas religiosas, políticas, comerciais ou qualquer outra atividade incompatível com as atividades profissionais.

- É proibida a interrupção intencional, interferências, monitoração, bloqueio e desligamento dos recursos da CPTM por pessoas não autorizadas.

- É proibido o envio, recuperação, acesso, exibição, armazenamento, impressão ou disseminação de materiais ou informações fraudulentas, coercitivas, ameaçadoras, ilícitas, racistas, de conotações sexuais ou obscenas, intimidatórias, difamatórias ou, de qualquer maneira, em desacordo com uma correta conduta profissional.

- É dever do usuário encerrar a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo.

- A CPTM deve ser informada sobre qualquer situação que configure violação de sigilo ou que possa colocar em risco a segurança, inclusive se relacionada a terceiros.

4.4. Cláusulas obrigatórias em contratos com terceiros

a) Cláusulas de submissão à Política e Normas de Segurança da Informação:

- ✓ Deve constar das propostas e/ou contratos com fornecedores, prestadores de serviços e parceiros, cláusula de conformidade com a Política e Normas de Segurança da Informação.

b) Cláusulas de sigilo, proteção e contraespionagem:

- ✓ Em todo contrato firmado com terceiros deverão constar cláusulas para proteção das informações da CPTM, e das informações sob sua custódia - de forma padronizada, a fim de garantir que todos os softwares e hardwares fornecidos serão livres de programas de espionagem (backdoors).

4.5. Descarte de Informações

- Toda informação, independentemente da mídia em que estiver armazenada, deverá ser descartada respeitando os prazos legais e conforme acordado com seu proprietário, observadas as políticas e normas vigentes.
- Em caso de descarte definitivo, as mídias deverão ser inutilizadas previamente.
- Em caso de reutilização, as mídias deverão ser submetidas a processos de limpeza para evitar a recuperação das informações gravadas anteriormente.

4.6. Registro de Incidentes

- Incidentes de segurança que forem registrados serão analisados e tratados em conformidade ao risco que represente à CPTM, podendo ser informados internamente pelos gestores de dados e/ou qualquer empregado da CPTM ou informados por entidades externas que envolvam a CPTM.
- Nos casos que envolvam qualquer incidente com dados pessoais, as áreas deverão comunicar imediatamente o Departamento de Privacidade e Proteção de Dados - DRPD.

5. ATUALIZAÇÕES

A CPTM revisitará a presente Política periodicamente e promoverá modificações sempre que necessário.

6. PROPONENTE

A Diretoria Administrativa e Financeira - DF e a Gerência de Tecnologia da Informação - GFI são responsáveis por esta Política.

7. DISPOSIÇÕES FINAIS

A CPTM promoverá continuamente, por meio de programas de comunicação e capacitação, ações de divulgação e conscientização de uma cultura de segurança da informação.
Esta Política, se aplica imediatamente, a partir de sua publicação.

8. REFERÊNCIAS

- Lei Federal nº 13.303/2016;
- Lei Federal nº 12.527/2011;
- Decreto Estadual nº 58.052/2012;
- Lei Federal n.º 12.527/2011;
- Lei Federal nº 6.404/1976;
- Estatuto Social da CPTM;
- Código de Conduta e Integridade – CCI;
- Código de Conduta e Integridade dos Fornecedores, Prestadores de Serviço e Parceiros da CPTM - CCIFPSP.

9. CONTROLE DE VERSÕES

Versão	Data	Pág.	Motivo
01	14/12/2020	Todas	RD 15562 de 10/12/2020 RCA 017 de 14/12/2020 Em cumprimento à Lei Federal 13.303/2016 e Estatuto Social da CPTM. A Diretoria Administrativa e Financeira é responsável por esta Política.
02	De acordo com o item 7	Todas	PRD PR 007 DE 02/02/204; RD 16946 DE 08/02/2024; PCA 005/2024 DE 09/02/2024; RCA 141 DE 20/02/2024; Parecer jurídico - FD.DRJP.118/2023 - Gerência Jurídica e Relatório de Conformidade nº 239/2023 da Gerência de Conformidade, Controles Internos e Gestão de Riscos. Em cumprimento a Lei 13.303/2016 e Atualização na Companhia.

10. ÍNDICE