Política de Segurança de Comunicações para o Setor de Entretenimento e Mídia

Baseado no Framework NIST 800-53 (RMF)

2. Propósito

Estabelecer um processo formal para proteger as comunicações confidenciais e proprietárias do setor de entretenimento e mídia contra interceptação, acesso não autorizado e modificação, a fim de garantir a confidencialidade, integridade e disponibilidade das informações.

3. Escopo

Esta política se aplica a todas as comunicações do setor de entretenimento e mídia, incluindo:

- **Comunicação por email:** Mensagens de email internas e externas.
- **Comunicação por internet:** Navegação na web, transferência de arquivos e uso de aplicativos web.
- **Comunicação por telefone:** Chamadas telefônicas fixas e móveis, videoconferências e mensagens de texto.
- **Comunicação por satélite:** Transmissão de dados e voz via satélite.

4. Política

O setor de entretenimento e mídia se compromete a:

- **Implementar medidas de segurança para proteger as comunicações confidenciais:** Implementar medidas de segurança como criptografia, autenticação e autorização para proteger as comunicações confidenciais contra interceptação, acesso não autorizado e modificação.
- **Controlar o acesso às comunicações:** Implementar medidas de controle de acesso para restringir o acesso às comunicações confidenciais aos usuários autorizados.
- **Monitorar as comunicações:** Monitorar as comunicações para detectar atividades anormais e potenciais ameaças.
- **Responder a incidentes de segurança:** Estabelecer um processo para responder a incidentes de segurança de forma rápida e eficaz.

5. Procedimentos Relacionados

- **Criptografia:**
  - Implementar criptografia para proteger as comunicações confidenciais em trânsito e em repouso.
  - Usar algoritmos de criptografia fortes e aprovados pelo NIST.
- **Autenticação e autorização:**
  - Implementar mecanismos de autenticação e autorização para controlar o acesso às comunicações confidenciais.
  - Usar métodos de autenticação fortes, como senhas complexas ou autenticação multifator.
- **Monitoramento:**
  - Monitorar as comunicações para detectar atividades anormais e potenciais ameaças.
  - Usar ferramentas de monitoramento adequadas para identificar e bloquear atividades maliciosas.
- **Resposta a incidentes:**

- Estabelecer um processo para responder a incidentes de segurança de forma rápida e eficaz.
- Investigar a causa do incidente e tomar medidas para remediar o problema.
- Documentar o incidente e as medidas tomadas para remediá-lo.

6. Não Conformidade

O não cumprimento desta política poderá resultar em medidas disciplinares, incluindo advertência verbal, advertência escrita, suspensão ou rescisão de contrato.

7. Compromisso/Autoridade da Gestão

A alta gerência do setor de entretenimento e mídia se compromete a fornecer os recursos necessários para a implementação e o cumprimento desta política. A equipe de segurança da informação é responsável pela gestão e atualização da política.

8. Cronograma de Revisão

A política será revisada anualmente ou após um incidente de segurança cibernética significativo.

9. Definições

- **Comunicação confidencial:** Comunicação que contém informações confidenciais ou proprietárias que não devem ser divulgadas a terceiros não autorizados.
- **Criptografia:** Processo de conversão de dados em um formato que só pode ser lido por pessoas autorizadas.
- **Autenticação:** Processo de verificar a identidade de um usuário.
- **Autorização:** Processo de determinar quais recursos um usuário pode acessar.

- **Incidente de segurança:** Evento que pode causar perda, confidencialidade, integridade ou disponibilidade das informações.

Observações:

- Esta política é um exemplo e deve ser adaptada às necessidades específicas do setor de entretenimento e mídia.
- É importante consultar especialistas em segurança cibernética para a implementação da política.