Plantilla de Política de Ciberseguridad:

Introducción.

El riesgo de robo de datos, estafas y violaciones de seguridad puede tener un impacto perjudicial en los sistemas, la infraestructura tecnológica y la reputación de una empresa. Como resultado, [Nombre de la Empresa] ha creado esta política para ayudar a describir las medidas de seguridad implementadas para garantizar que la información permanezca segura y protegida.

Objetivo.

El propósito de esta política es (a) proteger los datos y la infraestructura de [Nombre de la Empresa], (b) describir los protocolos y directrices que rigen las medidas de seguridad cibernética, (c) definir las reglas para el uso personal y empresarial, y (d) enumerar el proceso disciplinario de la empresa por violaciones de políticas.

Alcance.

Esta política se aplica a todos los trabajadores remotos de [Nombre de la Empresa], empleados permanentes y de medio tiempo, contratistas independientes, voluntarios, proveedores, pasantes y/o cualquier persona con acceso a los sistemas electrónicos, información, software y/o hardware de la empresa.

Información confidencial.

[Nombre de la Empresa] define “Información confidencial" como:

* Información financiera inédita y clasificada.
* Información de clientes, proveedores y accionistas.
* Clientes potenciales y datos relacionados con las ventas.
* Patentes, procesos de negocio y/o nuevas tecnologías.
* Contraseñas, asignaciones e información personal de los empleados.
* Contratos de empresa y registros legales.

Seguridad del dispositivo.

Uso de la empresa.

Para garantizar la seguridad de todos los dispositivos e información proporcionados por la empresa, los empleados de [Nombre de la Empresa] deben:

* Mantener todos los dispositivos proporcionados por la empresa, incluidas tabletas, computadoras y dispositivos móviles, protegidos con contraseña (mínimo de 8 caracteres).
* Asegurar todos los dispositivos relevantes antes de abandonar su escritorio.
* Obtener autorización del Gerente de Oficina y/o Gerente de Inventario antes de retirar dispositivos de las instalaciones de la empresa.
* Abstenerse de compartir contraseñas privadas con compañeros de trabajo, conocidos personales, personal directivo y/o accionistas.
* Actualizar periódicamente los dispositivos con el software de seguridad más reciente.

Uso personal.

[Nombre de la Empresa] reconoce que es posible que se requiera que los empleados utilicen dispositivos personales para acceder a los sistemas de la empresa. En estos casos, los empleados deben reportar esta información a la gerencia para fines de mantenimiento de registros. Para garantizar que los sistemas de la empresa estén protegidos, todos los empleados deben:

* Mantener todos los dispositivos protegidos con contraseña (mínimo de 8 caracteres).
* Asegurarse de que todos los dispositivos personales utilizados para acceder a los sistemas relacionados con la empresa estén protegidos con contraseña.
* Instalar un software de antivirus con todas las funciones.
* Actualizar periódicamente el software antivirus.
* Bloquear todos los dispositivos en caso de dejarse desatendidos.
* Asegurarse de que los dispositivos estén protegidos en todo momento.
* Utilizar siempre redes seguras y privadas.

Seguridad del correo electrónico.

Proteger los sistemas de correo electrónico es una alta prioridad, ya que los correos electrónicos pueden provocar robo de datos, estafas y contener software malicioso como gusanos y errores. Por lo tanto, [Nombre de la Empresa] exige que todos los empleados:

* Verificar la legitimidad de cada correo electrónico, incluida la dirección de estos y el nombre del remitente.
* Evitar abrir correos electrónicos sospechosos, archivos adjuntos y hacer clic en enlaces.
* Buscar errores gramaticales importantes.
* Evitar títulos y enlaces “*clickbait*”.
* Comunicarse con el departamento de TI en relación con cualquier correo electrónico sospechoso.

Transferencia de datos.

[Nombre de la Empresa] reconoce los riesgos de seguridad que conlleva la transferencia de datos confidenciales interna y/o externamente. Para minimizar las posibilidades de robo de datos, todos los empleados deberán:

* Abstenerse de transferir información clasificada a empleados y terceros.
* Transferir datos confidenciales únicamente a través de las redes de [Nombre de la Empresa].
* Obtener la autorización necesaria de la alta dirección.
* Verificar el destinatario de la información y asegurarse de tener implementadas las medidas de seguridad adecuadas.
* Respetar la ley de protección de datos y el acuerdo de confidencialidad de [Nombre de la Empresa].
* Alertar inmediatamente al departamento de TI sobre cualquier infracción, software malicioso y/o estafa.

Acción disciplinaria.

La violación de esta política puede dar lugar a medidas disciplinarias, que pueden llegar hasta el despido. Los protocolos disciplinarios de [Nombre de la Empresa] se basan en la gravedad de la infracción. Las violaciones no intencionales sólo justifican una advertencia verbal, las violaciones frecuentes de la misma naturaleza pueden dar lugar a una advertencia por escrito y las violaciones intencionales pueden dar lugar a la suspensión y/o terminación, dependiendo de las circunstancias del caso.