CyberTex
Global Solutions

Security and Compliance Policy 2024.

CyberTex
Global Solutions

Security and Compliance Policy 2024

Introduction

This Security and Compliance Policy outlines the measures taken by our tech offshore outsourcing firm to ensure the security of client data and maintain regulatory compliance. Our company is committed to protecting the confidentiality, integrity, and availability of client data by implementing industry best practices and complying with applicable laws and regulations.

Scope

This policy applies to all employees, contractors, and third-party service providers who have access to our clients' data, regardless of their location. All employees are responsible for adhering to this policy and ensuring that their actions align with the security and compliance requirements set out in this policy.

Information Security

Our company employs the following security measures to protect client data:

- **Secure LAN Infrastructure:** Our company utilizes a secure LAN infrastructure to ensure the safety of our internal network. All external access is routed through VPN to enhance our network security.
- **Password Management:** The security of our clients' data is a top priority for us. To prevent unauthorized access, we employ strong passwords and enable two-factor authentication where applicable. All laptops used in development are equipped with strong passwords and two-factor authentication. We also utilize a password manager to securely store our passwords and use different passwords for each account.
- **Data Encryption:** To further bolster our security, we use full-disk encryption to encrypt our data. This ensures that data remains secure even if a laptop is lost or stolen. Additionally, we employ encrypted messaging platforms for communication with our clients.
- **Virtual Private Networks:** We also use virtual private networks (VPNs) to safeguard our internet traffic from various attacks such as hacking, interception, malware, and phishing.
- **Regular Backups:** We regularly back up our data to cloud-based storage services or external hard drives as an extra layer of protection.
- **Security Policies and Employee Training:** We have developed comprehensive security policies that outline how to handle sensitive data, and our employees receive training to ensure that they follow these policies to minimize security risks. Furthermore, we restrict access to client data only to the employees who require it to minimize the risk of unauthorized access or data breaches.

Physical Security Protocols

In addition to security policies, we have established set of protocols for physical security as well which are:

- **Secured Premises:** We have security cameras, access controls, and ID badges to restrict access to our premises.
- **Regular Risk Assessment:** We perform regular risk assessments to identify potential security risks and implement necessary measures to mitigate them. This includes reviewing our security policies, procedures, and systems regularly to ensure that they remain effective.
- **Employee Background Check:** We conduct background checks on all new employees to verify their identities and backgrounds. This helps us prevent insider threats and ensure that our employees are trustworthy and reliable.
- **Disaster Recovery Plan:** We have established a disaster recovery plan to ensure business continuity in the event of a natural disaster, cyber-attack, or any other unforeseen event. This includes procedures for backup and recovery, alternate communication channels, and disaster recovery testing to ensure that our systems remain operational even during a crisis.

Regulatory Compliance

Our company adheres to the following regulations and standards:

- **General Data Protection Regulation (GDPR):** We comply with GDPR requirements and ensure that all client data is processed lawfully, fairly, and transparently.
- **Payment Card Industry Data Security Standard (PCI DSS):** We comply with PCI DSS requirements and ensure that client payment card data is secure and protected from unauthorized access.
- **Health Insurance Portability and Accountability Act (HIPAA):** We comply with HIPAA requirements and ensure that client healthcare data is kept confidential and secure.

Conclusion

Our company is committed to maintaining the security and confidentiality of client data while ensuring compliance with applicable regulations and standards. We regularly review and update our security and compliance policies to ensure that they remain effective and up-to-date with the latest industry standards. All employees are required to adhere to this policy, and failure to comply may result in disciplinary action up to and including termination.

www.cybertexglobalsolutions.com

CyberTex
Global Solutions