AllSafe Cybersecurity Encryption Policy

Introduction

AllSafe Cybersecurity is a security firm protecting the data of multiple Fortune 500 companies from cyber threats, data breaches, and insider risks. Encryption is a critical safeguard for ensuring confidentiality and maintaining trust with our clients. This policy establishes clear requirements for encrypting sensitive company information to strengthen security and ensure proper and sufficient compliance across all parts of the companies data (National Cybersecurity Society, 2019).

Purpose

The purpose of this policy is simple, focusing one core topic - encryption. Encryption must be used to protect company and client data—whether it's stored within a data center, in transit across networks, as well as on devices managed by AllSafe. Using strong encryption lowers the risk of unauthorized access and helps us stay in compliance with regulations like GDPR, HIPAA, and PCI DSS (Fitchburg State University, 2024).

Scope

This policy applies to all employees, contractors, vendors, and third-party partners working with AllSafe Cybersecurity systems. As far as company infrastructure, the policy covers AllSafe owned servers, workstations, and mobile devices. This policy will also cover cloud environments and client-facing apps and services. We need to make sure that first and foremost our clients data is always protected using modern encryption methods (Augusta University, n.d.).

Policy Statement

AllSafe Cybersecurity requires the use of approved encryption methods to secure sensitive information. This policy statement will cover two main types of data that needs to be encrypted at all times. The first is “data at rest”, which includes databases, servers, and backups. The encryption policy for “data at rest” is that it must be encrypted with AES-256 or an equivalent method. All laptops and mobile devices must have full disk encryption enabled (University of Arkansas at Pine Bluff, n.d.).The second is “data in transit”, which is defined as data that is sent over the network. All “data in transit” must use TLS 1.3 or higher, HTTPS, or a secure company VPN. Emails with sensitive or client data must be encrypted using PGP keys that will be provided to each employee (National Cybersecurity Society, 2019). This brings us to our next subject; the encryption keys. All encryption keys must be created, stored, and rotated using centralized key management systems. Access to keys is strictly limited to authorized personnel. Compromised keys must be reported and revoked immediately (Augusta University, n.d.).

Roles and Responsibilities

We will split this section into three main parts. The first pertains to all AllSafe employees, second is the field/penetration testing department, and last is the CISO/security team. All employees must encrypt sensitive files and communications as required. Report any suspected violations immediately and attend mandatory security training each quarter. The penetration testing department will implement and maintain encryption technologies while out in the field. They will also be responsible for providing training and technical support to clients. The CISO/

Security team will oversee policy enforcement, review encryption standards annually, authorize exceptions, and conduct periodic audits (Fitchburg State University, 2024).

Enforcement and Compliance

This encryption policy is to be read and understood by each and every AllSafe employee. Violations of this policy may result in disciplinary action, up to and including termination of employment. Monthly audits and reviews will take place unexpectedly and employees are required to participate. This is extremely important as it ensures AllSafe Cybersecurity continues to meet client expectations and regulatory requirements (Douglas College, 2025).

Conclusion

Using proper encryption is a cornerstone of AllSafe Cybersecurity's mission to protect the data of our clients. All employees need to take this policy seriously and familiarize yourself with the encryption standards detailed within. By enforcing this policy, AllSafe will continue to provide the highest level of data protection for every client.

References

Augusta University. (n.d.). Encryption policy. Augusta University. https://www.augusta.edu/services/legal/policyinfo/policy/encryption-policy.pdf

Douglas College. (2025). APA (7th ed.) citation style guide: Government documents. Douglas College Library. https://guides.douglascollege.ca/APA-7/GovernmentDocs

Fitchburg State University. (2024, May 9). Encryption policy (Version 1.2) [PDF]. Fitchburg State University. https://www.fitchburgstate.edu/sites/default/files/documents/2023-03/Encryption-Policy.pdf

National Cybersecurity Society. (2019). Encryption policy template [PDF]. National Cybersecurity Society. https://nationalcybersecuritysociety.org/wp-content/uploads/2019/10/Encryption-Policy-Template-FINAL.pdf

University of Arkansas at Pine Bluff. (n.d.). Data encryption policy [PDF]. University of Arkansas at Pine Bluff. https://uapb.edu/wp-content/uploads/2024/05/Data-Encryption-Policy-Revised.pdf