**Data Encryption**

Data encryption at ACME Defense Contractors strictly ensures confidentiality and integrity by following strong encryption and hashing techniques. The business uses AES - Rijndael a block cipher algorithm for symmetric encryption, which helps the business securely exchange symmetric keys between two systems. Both the sender and the recipient will have the same key, which should be safely held and exchanged only through secure means. The business uses Diffie-Hellman an asymmetric encryption approach that establishes a secure communication channel for private keys, and the advantage of the Diffie-Hellman approach is that it has the benefit of generating a public and private key on both sides of the transaction but only shares the public key. For cryptographic hash functions, the business uses RACE Integrity Primitives Evaluation Message Digest (RIPEMD). It is essential to safeguard sensitive data in transit and at rest since it is vulnerable to attackers who develop innovative ways to hack the system and steal data. Data at rest is data that is not actively traveling from one area to another over a network, and it can be saved on hard drives, in the cloud, on laptops, servers, backups, and other storage devices. Encryption for data at rest might simply encrypt sensitive files before storing them. When data is in transit, it is actively traveling from one point to another over a network. Data in transit can be encrypted using Secure Sockets Layer (SSL), Hypertext Transfer Protocol Secure (HTTPS), or any other secure connection that aids in the protection of data in transit. Furthermore, unclassified constrained documents (CUI) must be encrypted in transit on all platforms and stored at rest on mobile devices. Data governed by the International Traffic in Arms Regulations (ITAR) that is stored or in transit in the cloud must be encrypted end-to-end (E2EE).