**Information Security Program**

**Introduction**

The purpose of this document is to ensure confidentiality, integrity, and availability of security and document the information policies, standards, guidelines, and procedures that serve as the cornerstone of the program at ACME Defense Contractors. All the principles are taken to safeguard the resources that fall under federal and state laws and regulations, such as the National Institute of Standards and Technology (NIST 800-12, 800-18, 800-30, and 800-171), the Department of Defense (DoD), the Committee on National Security Systems (CNSS 4009), the International Organization for Standardization (ISO 27000 Series), the Securities Exchange Act of 1934 (the “Exchange Act”), the Securities Act of 1933 (the “Securities Act”), and the Sarbanes-Oxley Act of 2002 (“Sarbanes-Oxley”).

The program intends to provide robust security that corresponds with and supports ACME Defense Contractors in achieving its goals and managing the business's systems, networking, accounting, R&D, customer service, computing environments, and human resources. Furthermore, reduce business risks through efficient risk management. The program establishes principles for initiating, implementing, maintaining, and enhancing the information security of the business.

This security program will support the business in protecting itself from unauthorized access, ensuring accuracy in information, and restricting access based on privilege. The chief executive officer (CEO) authorizes the chief information officer (CIO) to create the security program, and the CIO ensures that all business objectives are achieved and will prioritize and make decisions. The security program will be designed, implemented, and managed by an Information Security Officer (ISO).

**Scope**

The program applies to the whole organization, including the CEO, CFO, CIO, staff, temporary workers, contractors, and guests who have access to the company’s tangible and intangible assets, including sensitive data, software, hardware, and storage media. In addition, everyone must sign and acknowledge the information security policy to ensure compliance.

**Desired Policies**

1. Security Policy
2. Code & Ethics Policy
3. Email Policy
4. Privacy Policy
5. Internet Usage Policy
6. Acceptable Use Policy
7. Human Resource Policy