**Authentication & Access Control**

**Authentication**

User identification is verified in various ways at ACME Defense Contractors. The business follows MFA (also known as multi-factor authentication) with network and device verification to significantly boost security. When a user attempts to login into an account, the key requirement is to have a verified device connected to the ACME Wi-Fi Network, which confirms the login. The system then prompts the user to provide a username and passphrase, validate the captcha, and then approve the login attempt through MFA (multi-factor authentication). Users can utilize any multi-factor authentication technique, but only through partnered integrations such as Microsoft Authenticator, Google Authenticator, Bio-Key, or Authy.

**Access Control**

RBAC (Role-based access control) is used at ACME Defense Contractors. The administrator deals with assigning privileges based on the job title for everyone in the business. RBAC is extremely beneficial as it allows the administrator to define groups and regulate privileges based on the role, which makes permission management simple and uncomplicated, promotes user productivity, reduces insider threats, and improves security. Once the permissions are defined, the permissions are autonomous. RBAC benefits the firm by preventing low-level workers or third-party contractors from accessing confidential data. These rights can subsequently be altered, and specific users can be granted exclusive access. ACME audits permissions for accuracy on a regular basis.