#	NIST SP 800-171r2 Policy	Description
1	**Access Control Policy** NIST SP 800-171 Reference NIST Control: AC	To limit access to systems to authorized users who work on approved devices to process permitted transactions and functions.
2	**Awareness and Training Policy** NIST SP 800-171 Reference NIST Control: AT	To ensure users are educated on the policies, procedures, and standards related to the organization's security of systems.
3	**Audit and Accountability Policy** NIST SP 800-171 Reference NIST Control: AU	To create, protect, and retain audit records for the purpose of monitoring, analysis, investigation, and reporting.
4	**Configuration Management Policy** NIST SP 800-171 Reference NIST Control: CM	To establish and maintain baseline configurations for ORGANIZATION_NAME's systems.
5	**Identification and Authentication Policy** NIST SP 800-171 Reference NIST Control: IA	To identify system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to ORGANIZATION_NAME's systems.
6	**Incident Response Policy** NIST SP 800-171 Reference NIST Control: IR	To establish incident handling capabilities for ORGANIZATION_NAME's systems.
7	**Maintenance Policy** NIST SP 800-171 Reference NIST Control: MA	To provide maintenance on organizational systems and record of such maintenance.
8	**Media Protection Policy** NIST SP 800-171 Reference NIST Control: MP	To protect and secure system media, both paper and digital.
9	**Personnel Security Policy** NIST SP 800-171 Reference NIST Control: PS	To screen individuals who may have authorization to access organizational systems and protect those systems in the event of an individual's termination or transfer.
10	**Physical Protection Policy** NIST SP 800-171 Reference NIST Control: PE	To limit physical access to organizational systems and protect the physical facility of such organizational systems.

#	NIST SP 800-171r2 Policy	Description
11	**Risk Assessment Policy** NIST SP 800-171 Reference NIST Control: RA	To periodically assess the risk to organizational operations, organizational assets, and individuals.
12	**Security Assessment Policy** NIST SP 800-171 Reference NIST Control: CA	To assess the security controls of ORGANIZATION_NAME's systems periodically.
13	**System and Communications Protection Policy** NIST SP 800-171 Reference NIST Control: SC	To monitor, control, and protect the internal and external communications of systems within the organization.
14	**System and Information Integrity Policy** NIST SP 800-171 Reference NIST Control: SI	To monitor system security alerts and advisories and take action in response.