NIST 800-171 Compliance Checklist

Sourced and condensed from Controlled Unclassified Information (CUI) security firm Cuick Trak's guide, here is a comprehensive checklist to help you establish robust security policies and strengthen your organization's security posture.

These eight steps will streamline the process for meeting NIST SP 800-171 compliance requirements.

- ☐ Step 1: Identify your CUI

  Conduct a comprehensive assessment of the employees and devices accessing the types of CUI and note where the data is located.

- ☐ Step 2: Categorize your CUI data

  Using the NIST 800-171 Control Families, categorize the data your organization uses.

- ☐ Step 3: Perform a security assessment

  Conduct a holistic security assessment to gauge your current cybersecurity posture, identify vulnerabilities, and fix any noted gaps.

- ☐ Step 4: Develop baseline controls

  Establish baseline safeguards against external threats, develop your data protection strategy, and furnish endpoint protection to preempt cyber incidents.

- ☐ Step 5: Perform ongoing risk assessments

  Evaluate your existing security measures and identify areas for bolstering CUI protection.

☐ Step 6: Document your security plan

Document your security plan and update your plan with a date and revision number whenever standard updates are issued.

☐ Step 7: Create a response plan

Create a response plan to minimize downtime and ensure swift and cost-effective restoration of operations in the event of a security breach.

☐ Step 8: Educate employees

Disseminate this checklist to staff involved in your cybersecurity operations and immediately update them on any further changes to your procedures.