Offline Survey

Name **Due Date**

Applies To Third Parties

Instructions/Guidelines
If your response is No (or) N/A, please provide reasoning in the Comments section.

Access Control

AC-1)Does your organization have documented access control policy and procedures for authorizing and revoking access rights to information systems?*
If your response is No (or) N/A, please provide reasoning in the Comments section.

AC-2)Are there processes in place to grant and approve users access to systems and data?*
If your response is No (or) N/A, please provide reasoning in the Comments section.

AC-17)Is there a remote access policy and procedures for systems transmitting, processing, and storing data that has been approved by management?*
If your response is No (or) N/A, please provide reasoning in the Comments section.

Awareness and Training

AT-1)Does your organization have documented security and awareness training policy and procedures?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

AT-2)Is security awareness training required for all employees at least annually, including contractors?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

Audit and Accountability

AU-1)Does your organization have documented audit and accountability policy and procedures?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

Security Assessment and Authorization

CA-1)Does your organization have documented security assessment and authorization policy and procedures?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

CA-2)Are there security assessment plans that describe the scope of the assessments and procedures to determine the security control effectiveness?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

Supporting Documents

CA-7)Is there a continuous monitoring program implemented to facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

CA-8)Are external penetration testing conducted regularly to identify vulnerabilities and attack vectors?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

Supporting Documents

Configuration Management

CM-1)Does your organization have documented configuration management policy and procedures?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

CM-2)Are current baseline configuration of the information system developed, documented, and maintained under configuration control?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

CM-3)Is there a documented and implemented configuration change control program that logs all changes?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

Contingency Planning

CP-1)Does your organization have documented contingency planning policy and procedures?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

Identification and Authentication

IA-1)Does your organization have documented identification and authentication policy and procedures?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

Incident Response

IR-1)Does your organization have documented incident response policy and procedures?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

IR-6)Are there incident handling procedures that defines roles and responsibilities and how to report and respond to security events?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

Media Protection

MP-1)Does your organization have documented media protection policy and procedures?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

MP-6)Is there a media sanitization process that is applied to equipment prior to disposal, reuse, or release?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

Physical and Environmental Protection

PE-1)Does your organization have documented physical and environmental protection policy and procedures?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

PE-3)Are controls implemented that restricts physical access to buildings, sensitive areas, and hardware?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

PE-6)Are controls implemented that monitors the physical access?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

Personnel Security

PS-1)Does your organization have documented personnel security policy and procedures?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

Risk Assessment

RA-1)Does your organization have documented risk assessment policy and procedures?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

RA-5)Are internal vulnerability scans conducted regularly to identify vulnerabilities?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

System and Services Acquisition

SA-11)Are application security testing conducted regularly to identify vulnerabilities and attack vectors?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

Supporting Documents

System and Communications Protection

SC-1)Does your organization have documented system and communications protection policy and procedures?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

SC-5) Are denial of service protection mechanisms implemented?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

SC-8)Are cryptographic mechanisms implemented to recognize changes to information during transmission?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

SC-28)Are cryptographic mechanisms implemented to prevent unauthorized disclosure and modification of information at rest?*

If your response is No (or) N/A, please provide reasoning in the Comments section.

System and Information Integrity

SI-1) Does your organization have documented system and information integrity policy and procedures?*

If your response is No (or) N/A, please provide reasoning in the Comments section.