AICPA SOC 2 Criteria by Trust Principal

	Control Focus	AICPA SOC 2 Provided Criteria
CC1.1	Corporate Integrity	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.
CC1.2	Board Oversight	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3	Management Oversight	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4	Employee Development	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5	Employee Accountability	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
CC2.1	Internal Control Policies and Procedures	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
CC2.2	Internal Control Communication	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
CC2.3	External Control Communication	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.
CC3.1	Risk Management - Objectives	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
CC3.2	Risk Management - Risk Committee	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
CC3.3	Risk Management - Fraud Detection	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.

	Control Focus	AICPA SOC 2 Provided Criteria
CC3.4	Risk Management - Assessment	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.
CC4.1	Internal Control Auditing - Assessments	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
CC4.2	Internal Control Auditing - Assessment Oversight	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
CC5.1	Risk Mitigation Controls	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
CC5.2	IT General Controls	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
CC5.3	Internal Control Structure	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
CC6.1	Access Controls	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
CC6.2	Authorization Controls	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
CC6.3	Role Based Access Controls	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

	Control Focus	AICPA SOC 2 Provided Criteria
CC6.4	Physical Access Controls	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
CC6.5	Data Disposal Controls	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.
CC6.6	External Defense Controls	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7	Data Loss Prevention Controls	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
CC6.8	Threat Detection Controls	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.
CC7.1	System Monitoring Controls	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
CC7.2	Incident Response - Detection	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
CC7.3	Incident Response - Escalation	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
CC7.4	Incident Response - Policy	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
CC7.5	Incident Response - Recovery	The entity identifies, develops, and implements activities to recover from identified security incidents.

	Control Focus	AICPA SOC 2 Provided Criteria
CC8.1	Change Management	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
CC9.1	Risk Mitigation - Disaster Recovery	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2	Risk Mitigation - Vendor Mgmt.	The entity assesses and manages risks associated with vendors and business partners.
C1.1	Confidentiality Controls	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
C1.2	Data Disposal Controls	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.
A1.1	System Monitoring Controls	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.
A1.2	Disaster Recovery Controls	The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.
PI1.1	Processing Integrity	The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.
PI.2	Processing Integrity	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.
PI1.3	Processing Integrity	The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.
PI1.4	Processing Integrity	The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.

	Control Focus	AICPA SOC 2 Provided Criteria
PI1.5	Processing Integrity	The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.
P1.1	Privacy	The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.
P2.1	Privacy	The entity communicates choices available regarding the collection, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.
P3.1	Privacy	Personal information is collected consistent with the entity's objectives related to privacy.
P3.2	Privacy	For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.
P4.1	Privacy	The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.
P4.2	Privacy	The entity retains personal information consistent with the entity's objectives related to privacy.
P4.3	Privacy	The entity securely disposes of personal information to meet the entity's objectives related to privacy.

	Control Focus	AICPA SOC 2 Provided Criteria
P5.1	Privacy	The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.
P5.2	Privacy	The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.
P6.1	Privacy	The entity discloses personal information to third parties with the explicit consent of data subjects and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.
P6.2	Privacy	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.
P6.3	Privacy	The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.
P6.4	Privacy	The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as needed basis and takes corrective action, if necessary.
P6.5	Privacy	The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.

	Control Focus	AICPA SOC 2 Provided Criteria
P6.6	Privacy	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.
P6.7	Privacy	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.
P7.1	Privacy	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.
P8.1	Privacy	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.