SOC 2 - Trust Services Criteria

SOC 2 - Trust Services Criteria - Policies and Procedures

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for: Client Company

Prepared by: YourIT Company

Table of Contents

91	SOC 2 - Trust Services Criteria CC2.3.4 - Provides Separate Communication Lines
92	SOC 2 - Trust Services Criteria CC2.3.5 - Selects Relevant Method of Communication
93	SOC 2 - Trust Services Criteria CC2.3.6 - Communicates Objectives Related to Confidentiality and Changes to Those Objectives
94	SOC 2 - Trust Services Criteria CC2.3.7 - Communicates Objectives Related to Privacy and Changes to Those Objectives
95	SOC 2 - Trust Services Criteria CC2.3.8 - Communicates Incident Reporting Methods
96	SOC 2 - Trust Services Criteria CC2.3.9 - Communicates Information About System Operation and Boundaries
97	SOC 2 - Trust Services Criteria CC2.3.10 - Communicates System Objectives
98	SOC 2 - Trust Services Criteria CC2.3.11 - Communicates System Responsibilities
99	SOC 2 - Trust Services Criteria CC2.3.12 - Communicates Information on Reporting System Failures, Incidents, Concerns, and Other Matters
100	SOC 2 - Trust Services Criteria CC3.1 - COSO Principle 6: Risk Assessment
101	SOC 2 - Trust Services Criteria CC3.1.1 - Operations Objectives Reflect Management's Choices
102	SOC 2 - Trust Services Criteria CC3.1.2 - Considers Tolerances for Risk
103	SOC 2 - Trust Services Criteria CC3.1.3 - Includes Operations and Financial Performance Goals
104	SOC 2 - Trust Services Criteria CC3.1.4 - Forms a Basis for Committing of Resources
105	SOC 2 - Trust Services Criteria CC3.1.5 - External Financial Reporting Objectives Comply With Applicable Accounting Standards
106	SOC 2 - Trust Services Criteria CC3.1.6 - Considers Materiality
107	SOC 2 - Trust Services Criteria CC3.1.7 - Reflects Entity Activities
108	SOC 2 - Trust Services Criteria CC3.1.8 - External Nonfinancial Reporting Objectives Comply With Externally Established Frameworks
109	SOC 2 - Trust Services Criteria CC3.1.9 - Considers the Required Level of Precision
110	SOC 2 - Trust Services Criteria CC3.1.10 - Reflects Entity Activities
111	SOC 2 - Trust Services Criteria CC3.1.11 - Internal Reporting Objectives Reflect Management's Choices
112	SOC 2 - Trust Services Criteria CC3.1.12 - Considers the Required Level of Precision
113	SOC 2 - Trust Services Criteria CC3.1.13 - Reflects Entity Activities

114	SOC 2 - Trust Services Criteria CC3.1.14 - Compliance Objectives Reflect External Laws and Regulations
115	SOC 2 - Trust Services Criteria CC3.1.15 - Considers Tolerances for Risk
116	SOC 2 - Trust Services Criteria CC3.1.16 - Establishes Sub-Objectives for Risk Assessment
117	SOC 2 - Trust Services Criteria CC3.2 - COSO Principle 7: Risk Identification and Analysis
118	SOC 2 - Trust Services Criteria CC3.2.1 - Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels
119	SOC 2 - Trust Services Criteria CC3.2.2 - Analyzes Internal and External Factors
120	SOC 2 - Trust Services Criteria CC3.2.3 - Involves Appropriate Levels of Management
121	SOC 2 - Trust Services Criteria CC3.2.4 - Estimates Significance of Risks Identified
122	SOC 2 - Trust Services Criteria CC3.2.5 - Determines How to Respond to Risks
123	SOC 2 - Trust Services Criteria CC3.2.6 - Identifies Threats to Objectives
124	SOC 2 - Trust Services Criteria CC3.2.7 - Identifies Vulnerability of System Components
125	SOC 2 - Trust Services Criteria CC3.2.8 - Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other Parties
126	SOC 2 - Trust Services Criteria CC3.2.9 - Assesses the Significance of the Risks
127	SOC 2 - Trust Services Criteria CC3.3 - COSO Principle 8: Fraud Potential
128	SOC 2 - Trust Services Criteria CC3.3.1 - Considers Various Types of Fraud
129	SOC 2 - Trust Services Criteria CC3.3.2 - Assesses Incentives and Pressures
130	SOC 2 - Trust Services Criteria CC3.3.3 - Assesses Opportunities
131	SOC 2 - Trust Services Criteria CC3.3.4 - Assesses Attitudes and Rationalizations
132	SOC 2 - Trust Services Criteria CC3.3.5 - Considers the Risks Related to the Use of IT and Access to Information
133	SOC 2 - Trust Services Criteria CC3.4 - COSO Principle 9: Change Identification and Assessment
134	SOC 2 - Trust Services Criteria CC3.4.1 - Assesses Changes in the External Environment
135	SOC 2 - Trust Services Criteria CC3.4.2 - Assesses Changes in the Business Model

159	SOC 2 - Trust Services Criteria CC5.1.6 - Addresses Segregation of Duties
160	SOC 2 - Trust Services Criteria CC5.2 - COSO Principle 11: General Control Activities
161	SOC 2 - Trust Services Criteria CC5.2.1 - Determines Dependency Between the Use of Technology in Business Processes and Technology General Controls
162	SOC 2 - Trust Services Criteria CC5.2.2 - Relevant Technology Infrastructure Control Activities
163	SOC 2 - Trust Services Criteria CC5.2.3 - Relevant Security Management Process Controls Activities
164	SOC 2 - Trust Services Criteria CC5.2.4 - Relevant Technology Acquisition, Development, and Maintenance Process Control Activities
165	SOC 2 - Trust Services Criteria CC5.3 - COSO Principle 12: Policies & Procedures
166	SOC 2 - Trust Services Criteria CC5.3.1 - Establishes Policies and Procedures to Support Deployment of Management's Directives
167	SOC 2 - Trust Services Criteria CC5.3.2 - Establishes Responsibility and Accountability for Executing Policies and Procedures
168	SOC 2 - Trust Services Criteria CC5.3.3 - Performs in a Timely Manner
169	SOC 2 - Trust Services Criteria CC5.3.4 - Takes Corrective Action
170	SOC 2 - Trust Services Criteria CC5.3.5 - Performs Using Competent Personnel
171	SOC 2 - Trust Services Criteria CC5.3.6 - Reassesses Policies and Procedures
172	SOC 2 - Trust Services Criteria CC6.1 - Logical and Physical Access Controls
173	SOC 2 - Trust Services Criteria CC6.1.1 - Identifies and Manages the Inventory of Information Assets
174	SOC 2 - Trust Services Criteria CC6.1.2 - Assesses New Architectures
175	SOC 2 - Trust Services Criteria CC6.1.3 - Restricts Logical Access
176	SOC 2 - Trust Services Criteria CC6.1.4 - Identifies and Authenticates Users
177	SOC 2 - Trust Services Criteria CC6.1.5 - Considers Network Segmentation
178	SOC 2 - Trust Services Criteria CC6.1.6 - Manages Points of Access
179	SOC 2 - Trust Services Criteria CC6.1.7 - Restricts Access to Information Assets
180	SOC 2 - Trust Services Criteria CC6.1.8 - Manages Identification and Authentication

181	SOC 2 - Trust Services Criteria CC6.1.9 - Manages Credentials for Infrastructure and Software
182	SOC 2 - Trust Services Criteria CC6.1.10 - Uses Encryption to Protect Data
183	SOC 2 - Trust Services Criteria CC6.1.11 - Protects Cryptographic Keys
184	SOC 2 - Trust Services Criteria CC6.1.12 - Restricts Access to and Use of Confidential Information for Identified Purposes
185	SOC 2 - Trust Services Criteria CC6.1.13 - Restricts Access to and the Use of Personal Information
186	SOC 2 - Trust Services Criteria CC6.2 - User Registration, Authorization, and Termination
187	SOC 2 - Trust Services Criteria CC6.2.1 - Creates Access Credentials to Protected Information Assets
188	SOC 2 - Trust Services Criteria CC6.2.2 - Reviews Validity of Access Credentials
189	SOC 2 - Trust Services Criteria CC6.2.3 - Prevents the Use of Credentials When No Longer Valid
190	SOC 2 - Trust Services Criteria CC6.3 - Least Privilege and Segregation of Duties
191	SOC 2 - Trust Services Criteria CC6.3.1 - Creates or Modifies Access to Protected Information Assets
192	SOC 2 - Trust Services Criteria CC6.3.2 - Removes Access to Protected Information Assets
193	SOC 2 - Trust Services Criteria CC6.3.3 - Uses Access Control Structures
194	SOC 2 - Trust Services Criteria CC6.3.4 - Reviews Access Roles and Rules
195	SOC 2 - Trust Services Criteria CC6.4 - Physical Access Restrictions
196	SOC 2 - Trust Services Criteria CC6.4.1 - Creates or Modifies Physical Access
197	SOC 2 - Trust Services Criteria CC6.4.2 - Removes Physical Access
198	SOC 2 - Trust Services Criteria CC6.4.3 - Reviews Physical Access
199	SOC 2 - Trust Services Criteria CC6.5 - Discontinues Protections
200	SOC 2 - Trust Services Criteria CC6.5.1 - Removes Data and Software From Entity Control
201	SOC 2 - Trust Services Criteria CC6.6 - Logical Access
202	SOC 2 - Trust Services Criteria CC6.6.1 - Restricts Access
203	SOC 2 - Trust Services Criteria CC6.6.2 - Protects Identification and Authentication Credentials

204	SOC 2 - Trust Services Criteria CC6.6.3 - Requires Additional Authentication or Credentials
205	SOC 2 - Trust Services Criteria CC6.6.4 - Implements Boundary Protection Systems
206	SOC 2 - Trust Services Criteria CC6.7 - Information Restrictions
207	SOC 2 - Trust Services Criteria CC6.7.1 - Restricts the Ability to Perform Transmission
208	SOC 2 - Trust Services Criteria CC6.7.2 - Uses Encryption Technologies or Secure Communication Channels to Protect Data
209	SOC 2 - Trust Services Criteria CC6.7.3 - Protects Removal Media
210	SOC 2 - Trust Services Criteria CC6.7.4 - Protects Endpoint Devices
211	SOC 2 - Trust Services Criteria CC6.8 - Unauthorized or Malicious Software
212	SOC 2 - Trust Services Criteria CC6.8.1 - Restricts Installation and Modification of Application and Software
213	SOC 2 - Trust Services Criteria CC6.8.2 - Detects Unauthorized Changes to Software and Configuration Parameters
214	SOC 2 - Trust Services Criteria CC6.8.3 - Uses a Defined Change Control Process
215	SOC 2 - Trust Services Criteria CC6.8.4 - Uses Antivirus and Anti-Malware Software
216	SOC 2 - Trust Services Criteria CC6.8.5 - Scans Information Assets from Outside the Entity for Malware and Other Unauthorized Software
217	SOC 2 - Trust Services Criteria CC7.1 - System Operations
218	SOC 2 - Trust Services Criteria CC7.1.1 - Uses Defined Configuration Standards
219	SOC 2 - Trust Services Criteria CC7.1.2 - Monitors Infrastructure and Software
220	SOC 2 - Trust Services Criteria CC7.1.3 - Implements Change-Detection Mechanisms
221	SOC 2 - Trust Services Criteria CC7.1.4 - Detects Unknown or Unauthorized Components
222	SOC 2 - Trust Services Criteria CC7.1.5 - Conducts Vulnerability Scans
223	SOC 2 - Trust Services Criteria CC7.2 - Monitors Systems
224	SOC 2 - Trust Services Criteria CC7.2.1 - Implements Detection Policies, Procedures, and Tools
225	SOC 2 - Trust Services Criteria CC7.2.2 - Designs Detection Measures
226	SOC 2 - Trust Services Criteria CC7.2.3 - Implements Filters to Analyze Anomalies

227	SOC 2 - Trust Services Criteria CC7.2.4 - Monitors Detection Tools for Effective Operation
228	SOC 2 - Trust Services Criteria CC7.3 - Evaluates Security Events
229	SOC 2 - Trust Services Criteria CC7.3.1 - Responds to Security Incidents
230	SOC 2 - Trust Services Criteria CC7.3.2 - Communicates and Reviews Detected Security Events
231	SOC 2 - Trust Services Criteria CC7.3.3 - Develops and Implements Procedures to Analyze Security Incidents
232	SOC 2 - Trust Services Criteria CC7.3.4 - Assesses the Impact on Confidential Information
233	SOC 2 - Trust Services Criteria CC7.3.5 - Determines Confidential Information Used or Disclosed
234	SOC 2 - Trust Services Criteria CC7.3.6 - Assesses the Impact on Personal Information
235	SOC 2 - Trust Services Criteria CC7.3.7 - Determines Personal Information Used or Disclosed
236	SOC 2 - Trust Services Criteria CC7.4 - Incident Response
237	SOC 2 - Trust Services Criteria CC7.4.1 - Assigns Roles and Responsibilities
238	SOC 2 - Trust Services Criteria CC7.4.2 - Contains and Responds to Security Incidents
239	SOC 2 - Trust Services Criteria CC7.4.3 - Mitigates Ongoing Security Incidents
240	SOC 2 - Trust Services Criteria CC7.4.4 - Resolves Security Incidents
241	SOC 2 - Trust Services Criteria CC7.4.5 - Restores Operations
242	SOC 2 - Trust Services Criteria CC7.4.6 - Develops and Implements Communication of Security Incidents
243	SOC 2 - Trust Services Criteria CC7.4.7 - Obtains Understanding of Nature of Incident and Determines Containment Strategy
244	SOC 2 - Trust Services Criteria CC7.4.8 - Remediates Identified Vulnerabilities
245	SOC 2 - Trust Services Criteria CC7.4.9 - Communicates Remediation Activities
246	SOC 2 - Trust Services Criteria CC7.4.10 - Evaluates the Effectiveness of Incident Response
247	SOC 2 - Trust Services Criteria CC7.4.11 - Periodically Evaluates Incidents
248	SOC 2 - Trust Services Criteria CC7.4.12 - Applies Breach Response Procedures
249	SOC 2 - Trust Services Criteria CC7.4.13 - Communicates Unauthorized Use and Disclosure

250	SOC 2 - Trust Services Criteria CC7.4.14 - Application of Sanctions
251	SOC 2 - Trust Services Criteria CC7.5 - Recovery from Incidents
252	SOC 2 - Trust Services Criteria CC7.5.1 - Restores the Affected Environment
253	SOC 2 - Trust Services Criteria CC7.5.2 - Communicates Information About the Incident
254	SOC 2 - Trust Services Criteria CC7.5.3 - Determines Root Cause of the Event
255	SOC 2 - Trust Services Criteria CC7.5.4 - Implements Changes to Prevent and Detect Recurrences
256	SOC 2 - Trust Services Criteria CC7.5.5 - Improves Response and Recovery Procedures
257	SOC 2 - Trust Services Criteria CC7.5.6 - Implements Incident Recovery Plan Testing
258	SOC 2 - Trust Services Criteria CC8.1 - Change Management
259	SOC 2 - Trust Services Criteria CC8.1.1 - Manages Changes Throughout the System Lifecycle
260	SOC 2 - Trust Services Criteria CC8.1.2 - Authorizes Changes
261	SOC 2 - Trust Services Criteria CC8.1.3 - Designs and Develops Changes
262	SOC 2 - Trust Services Criteria CC8.1.4 - Documents Changes
263	SOC 2 - Trust Services Criteria CC8.1.5 - Tracks System Changes
264	SOC 2 - Trust Services Criteria CC8.1.6 - Configures Software
265	SOC 2 - Trust Services Criteria CC8.1.7 - Tests System Changes
266	SOC 2 - Trust Services Criteria CC8.1.8 - Approves System Changes
267	SOC 2 - Trust Services Criteria CC8.1.9 - Deploys System Changes
268	SOC 2 - Trust Services Criteria CC8.1.10 - Identifies and Evaluates System Changes
269	SOC 2 - Trust Services Criteria CC8.1.11 - Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents
270	SOC 2 - Trust Services Criteria CC8.1.12 - Creates Baseline Configuration of IT Technology
271	SOC 2 - Trust Services Criteria CC8.1.13 - Provides for Changes Necessary in Emergency Situations
272	SOC 2 - Trust Services Criteria CC8.1.14 - Protects Confidential Information
273	SOC 2 - Trust Services Criteria CC8.1.15 - Manages Patch Changes
274	SOC 2 - Trust Services Criteria CC8.1.16 - Considers System Resilience

275	SOC 2 - Trust Services Criteria CC8.1.17 - Protects Confidential Information
276	SOC 2 - Trust Services Criteria CC8.1.18 - Protects Personal Information
277	SOC 2 - Trust Services Criteria CC8.1.19 - Privacy by Design
278	SOC 2 - Trust Services Criteria CC9.1 - Risk Mitigation
279	SOC 2 - Trust Services Criteria CC9.1.1 - Considers Mitigation of Risks of Business Disruption
280	SOC 2 - Trust Services Criteria CC9.1.2 - Considers the Use of Insurance to Mitigate Financial Impact Risks
281	SOC 2 - Trust Services Criteria CC9.2 - Third Party Risk Management
282	SOC 2 - Trust Services Criteria CC9.2.1 - Establishes Requirements for Vendor and Business Partner Engagements
283	SOC 2 - Trust Services Criteria CC9.2.2 - Identifies Third-Party Vulnerabilities
284	SOC 2 - Trust Services Criteria CC9.2.3 - Assesses Vendor and Business Partner Risks
285	SOC 2 - Trust Services Criteria CC9.2.4 - Assigns Responsibility and Accountability for Managing Vendors and Business Partners
286	SOC 2 - Trust Services Criteria CC9.2.5 - Establishes Communication Protocols for Vendors and Business Partners
287	SOC 2 - Trust Services Criteria CC9.2.6 - Establishes Exception Handling Procedures From Vendors and Business Partners
288	SOC 2 - Trust Services Criteria CC9.2.7 - Assesses Vendor and Business Partner Performance
289	SOC 2 - Trust Services Criteria CC9.2.8 - Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments
290	SOC 2 - Trust Services Criteria CC9.2.9 - Implements Procedures for Terminating Vendor and Business Partner Relationships
291	SOC 2 - Trust Services Criteria CC9.2.10 - Obtains Confidentiality Commitments from Vendors and Business Partners
292	SOC 2 - Trust Services Criteria CC9.2.11 - Assesses Compliance With Confidentiality Commitments of Vendors and Business Partners
293	SOC 2 - Trust Services Criteria CC9.2.12 - Obtains Privacy Commitments from Vendors and Business Partners
294	SOC 2 - Trust Services Criteria CC9.2.13 - Assesses Compliance with Privacy Commitments of Vendors and Business Partners
295	SOC 2 - Trust Services Criteria P1.0 - Additional Criteria for Privacy - Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy
296	SOC 2 - Trust Services Criteria P1.1 - Privacy Notice

297	SOC 2 - Trust Services Criteria P1.1.1 - Communicates to Data Subjects
298	SOC 2 - Trust Services Criteria P1.1.2 - Provides Notice to Data Subjects [C]
299	SOC 2 - Trust Services Criteria P1.1.3 - Covers Entities and Activities in Notice [C]
300	SOC 2 - Trust Services Criteria P1.1.4 - Uses Clear Language and Presents a Current Privacy Notice in a Location Easily Found by Data Subjects [C]
301	SOC 2 - Trust Services Criteria P1.1.5 - Reviews the Privacy Notice [C]
302	SOC 2 - Trust Services Criteria P1.1.6 - Communicates Changes to Notice [C]
303	SOC 2 - Trust Services Criteria P1.1.7 - Retains Prior Notices [C]
304	SOC 2 - Trust Services Criteria P2.0 - Privacy Criteria Related to Choice and Consent
305	SOC 2 - Trust Services Criteria P2.1 - Communications with Data Subjects
306	SOC 2 - Trust Services Criteria P2.1.1 - Communicates to Data Subjects [C]
307	SOC 2 - Trust Services Criteria P2.1.2 - Communicates Consequences of Denying or Withdrawing Consent [C]
308	SOC 2 - Trust Services Criteria P2.1.3 - Obtains Implicit or Explicit Consent [C]
309	SOC 2 - Trust Services Criteria P2.1.4 - Documents and Obtains Consent for New Purposes and Uses [C]
310	SOC 2 - Trust Services Criteria P2.1.5 - Obtains Explicit Consent for Sensitive Information [C]
311	SOC 2 - Trust Services Criteria P2.1.6 - Obtains Consent for Data Transfers [C]
312	SOC 2 - Trust Services Criteria P3.0 - Privacy Criteria Related to Collection
313	SOC 2 - Trust Services Criteria P3.1 - Personal Information Collection
314	SOC 2 - Trust Services Criteria P3.1.1 - Limits the Collection of Personal Information [P][C]
315	SOC 2 - Trust Services Criteria P3.1.2 - Collects Information by Fair and Lawful Means [P][C]
316	SOC 2 - Trust Services Criteria P3.1.3 - Collects Information From Reliable Sources [P][C]
317	SOC 2 - Trust Services Criteria P3.1.4 - Informs Data Subjects When Additional Information Is Acquired [P][C]
318	SOC 2 - Trust Services Criteria P3.2 - Explicit Consent

319	SOC 2 - Trust Services Criteria P3.2.1 - Informs Data Subjects of Consequences of Failure to Provide Consent [C]
320	SOC 2 - Trust Services Criteria P3.2.2 - Documents Explicit Consent to Retain Information [C]
321	SOC 2 - Trust Services Criteria P4.0 - Privacy Criteria Related to Use, Retention, and Disposal
322	SOC 2 - Trust Services Criteria P4.1 - Limits Use
323	SOC 2 - Trust Services Criteria P4.1.1 - Uses Personal Information for Intended Purposes [P][C]
324	SOC 2 - Trust Services Criteria P4.2 - Retention
325	SOC 2 - Trust Services Criteria P4.2.1 - Retains Personal Information [P][C]
326	SOC 2 - Trust Services Criteria P4.2.2 - Protects Personal Information [P][C]
327	SOC 2 - Trust Services Criteria P4.3 - Disposal
328	SOC 2 - Trust Services Criteria P4.3.1 - Captures, Identifies, and Flags Requests for Deletion [P][C]
329	SOC 2 - Trust Services Criteria P4.3.2 - Disposes of, Destroys, and Redacts Personal Information [P][C]
330	SOC 2 - Trust Services Criteria P4.3.3 - Destroys Personal Information [P][C]
331	SOC 2 - Trust Services Criteria P5.0 - Privacy Criteria Related to Access
332	SOC 2 - Trust Services Criteria P5.1 - Access
333	SOC 2 - Trust Services Criteria P5.1.1 - Responds to Data Controller Requests [P]
334	SOC 2 - Trust Services Criteria P5.1.2 - Authenticates Data Subjects' Identity [P][C]
335	SOC 2 - Trust Services Criteria P5.1.3 - Permits Data Subjects Access to Their Personal Information [P][C]
336	SOC 2 - Trust Services Criteria P5.1.4 - Provides Understandable Personal Information Within Reasonable Time [P][C]
337	SOC 2 - Trust Services Criteria P5.1.5 - Informs Data Subjects If Access Is Denied [P][C]
338	SOC 2 - Trust Services Criteria P5.2 - Corrections and Amendments
339	SOC 2 - Trust Services Criteria P5.2.1 - Responds to Data Controller Requests [P]
340	SOC 2 - Trust Services Criteria P5.2.2 - Communicates Denial of Access Requests [P][C]
341	SOC 2 - Trust Services Criteria P5.2.3 - Permits Data Subjects to Update or Correct Personal Information [P][C]

342	SOC 2 - Trust Services Criteria P5.2.4 - Communicates Denial of Correction Requests [P][C]
343	SOC 2 - Trust Services Criteria P6.0 - Privacy Criteria Related to Disclosure and Notification
344	SOC 2 - Trust Services Criteria P6.1 - Third Parties
345	SOC 2 - Trust Services Criteria P6.1.1 - Communicates Privacy Policies to Third Parties [P][C]
346	SOC 2 - Trust Services Criteria P6.1.2 - Discloses Personal Information Only When Appropriate [P][C]
347	SOC 2 - Trust Services Criteria P6.1.3 - Discloses Personal Information Only to Appropriate Third Parties [P][C]
348	SOC 2 - Trust Services Criteria P6.1.4 - Discloses Information to Third Parties for New Purposes and Uses [P][C]
349	SOC 2 - Trust Services Criteria P6.2 - Authorized Disclosures
350	SOC 2 - Trust Services Criteria P6.2.1 - Creates and Retains Record of Authorized Disclosures [P][C]
351	SOC 2 - Trust Services Criteria P6.3 - Unauthorized Disclosures
352	SOC 2 - Trust Services Criteria P6.3.1 - Creates and Retains Record of Detected or Reported Unauthorized Disclosures [P] [C]
353	SOC 2 - Trust Services Criteria P6.4 - Vendor and Third Party Privacy Commitments
354	SOC 2 - Trust Services Criteria P6.4.1 - Evaluates Third-Party Compliance With Privacy Commitments [P][C]
355	SOC 2 - Trust Services Criteria P6.4.2 - Remediates Misuse of Personal Information by a Third Party [P][C]
356	SOC 2 - Trust Services Criteria P6.4.3 - Obtains Commitments to Report Unauthorized Disclosures [P][C]
357	SOC 2 - Trust Services Criteria P6.5 - Vendor and Third Party Unauthorized Disclosures
358	SOC 2 - Trust Services Criteria P6.5.1 - Remediates Misuse of Personal Information by a Third Party [P][C]
359	SOC 2 - Trust Services Criteria P6.5.2 - Reports Actual or Suspected Unauthorized Disclosures [P][C]
360	SOC 2 - Trust Services Criteria P6.6 - Breach Notification
361	SOC 2 - Trust Services Criteria P6.6.1 - Identifies Reporting Requirements [P][C]
362	SOC 2 - Trust Services Criteria P6.6.2 - Provides Notice of Breaches and Incidents [P][C]
363	SOC 2 - Trust Services Criteria P6.7 - Accounting of Storage and Disclosure
364	SOC 2 - Trust Services Criteria P6.7.1 - Responds to Data Controller Requests [P]

365	SOC 2 - Trust Services Criteria P6.7.2 - Identifies Types of Personal Information and Handling Process [P][C]
366	SOC 2 - Trust Services Criteria P6.7.3 - Captures, Identifies, and Communicates Requests for Information [P][C]
367	SOC 2 - Trust Services Criteria P7.0 - Privacy Criteria Related to Quality
368	SOC 2 - Trust Services Criteria P7.1 - Data Quality
369	SOC 2 - Trust Services Criteria P7.1.1 - Ensures Accuracy and Completeness of Personal Information [P][C] —
370	SOC 2 - Trust Services Criteria P7.1.2 - Ensures Relevance of Personal Information [P][C]
371	SOC 2 - Trust Services Criteria P8.0 - Privacy Criteria Related to Monitoring and Enforcement
372	SOC 2 - Trust Services Criteria P8.1 - Communications
373	SOC 2 - Trust Services Criteria P8.1.1 - Communicates to Data Subjects or Data Controllers [P][C]
374	SOC 2 - Trust Services Criteria P8.1.2 - Addresses Inquiries, Complaints, and Disputes [P][C]
375	SOC 2 - Trust Services Criteria P8.1.3 - Documents and Communicates Dispute Resolution and Recourse [P][C]
376	SOC 2 - Trust Services Criteria P8.1.4 - Documents and Reports Compliance Review Results [P][C]
377	SOC 2 - Trust Services Criteria P8.1.5 - Documents and Reports Instances of Noncompliance [P][C]
378	SOC 2 - Trust Services Criteria P8.1.6 - Performs Ongoing Monitoring [P][C]
379	SOC 2 - Trust Services Criteria PI1.1 - Additional Criteria for Processing Integrity (Over the Provision of Services or the Production, Manufacturing, or Distribution of Goods)
380	SOC 2 - Trust Services Criteria PI1.1.1 - Identifies Functional and Nonfunctional Requirements and Information Specifications
381	SOC 2 - Trust Services Criteria PI1.1.2 - Defines Data Necessary to Support a Product or Service
382	SOC 2 - Trust Services Criteria PI1.1.3 - Data Definition Components
383	SOC 2 - Trust Services Criteria PI1.1.4 - Data Definition Accuracy
384	SOC 2 - Trust Services Criteria PI1.1.5 - Data Description
385	SOC 2 - Trust Services Criteria PI1.2 - Defines Information Necessary to Support the Use of a Good or Product
386	SOC 2 - Trust Services Criteria PI1.2.1 - Defines Characteristics of Processing Inputs
387	SOC 2 - Trust Services Criteria PI1.2.3 - Evaluates Processing Inputs

388	SOC 2 - Trust Services Criteria PI1.2.4 - Creates and Maintains Records of System Inputs
389	SOC 2 - Trust Services Criteria PI1.3 - System Processing Policies & Procedures
390	SOC 2 - Trust Services Criteria PI1.3.1 - Defines Processing Specifications
391	SOC 2 - Trust Services Criteria PI1.3.2 - Defines Processing Activities
392	SOC 2 - Trust Services Criteria PI1.3.3 - Detects and Corrects Processing or Production Activity Errors
393	SOC 2 - Trust Services Criteria PI1.3.4 - Records System Processing Activities
394	SOC 2 - Trust Services Criteria PI1.3.5 - Processes Inputs
395	SOC 2 - Trust Services Criteria PI1.4 - Process Output Policies and Procedures
396	SOC 2 - Trust Services Criteria PI1.4.1 - Protects Output
397	SOC 2 - Trust Services Criteria PI1.4.2 - Distributes Output Only to Intended Parties
398	SOC 2 - Trust Services Criteria PI1.4.3 - Distributes Output Completely and Accurately
399	SOC 2 - Trust Services Criteria PI1.4.4 - Creates and Maintains Records of System Output Activities
400	SOC 2 - Trust Services Criteria PI1.5 - Storage Policies and Procedures
401	SOC 2 - Trust Services Criteria PI1.5.1 - Protects Stored Items
402	SOC 2 - Trust Services Criteria PI1.5.2 - Archives and Protects System Records
403	SOC 2 - Trust Services Criteria PI1.5.3 - Stores Data Completely and Accurately
404	SOC 2 - Trust Services Criteria PI1.5.4 - Creates and Maintains Records of System Storage Activities

Purpose

SOC for Service Organizations are internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service. SOC is a standard of the American Institute of Certified Public Accountants (AICPA) and audits must be performed by CPA firms.

The Trust Services Criteria is to be used when evaluating the suitability of the design and operating effectiveness of controls relevant to the security, availability, or processing integrity of information and systems used to provide products or services, or the confidentiality or privacy of information processed by the systems used to provide products or services at an entity, a division, or an operating unit of an entity.

In addition, the Trust Services Criteria may be used when evaluating the design and operating effectiveness of controls relevant to the security, availability, processing integrity, confidentiality or privacy of a particular type of information processed by one or more of an entity's systems or one or more systems used to support a particular function within the entity.

The Trust Services Criteria set forth the outcomes that an entity's controls should ordinarily meet to achieve the entity's unique objectives. Therefore, the Trust Services Criteria are intended to be used for evaluation and reporting, regardless of the specific controls implemented by management. This contrasts with the approach taken by process and controls frameworks, which mandate that the entity implement a specific set of controls. The Trust Services Criteria recognize that there is no specific set of processes and controls that can effectively mitigate all the unique threats, vulnerabilities, and risks that entities face.

Instead, each entity is responsible for establishing its own objectives, assessing the unique risks that threaten the achievement of those objectives, and implementing processes and controls to mitigate those risks to acceptable levels. Because each entity is unique, applying the Trust Services Criteria in actual situations requires judgment.

Source: AICPS TSP Section 100 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (with Revised Points of Focus 2022)

Scope

This policy applies to the workforce members and vendors of entities that are third-party outsourced service organizations.

Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

SOC 2 - Trust Services Criteria A1.1 - Additional Criteria for Availability

SOC 2 - Trust Services Criteria	Other Requirements
A1.1 Additional Criteria for Availability	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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.

Guidance
The entity must maintain, monitor, and evaluate 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. Laws, regulations, contracts, and insurance policies should be reviewed for specific requirements.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- TSC-A1.1 - Availability: Maintain, monitor, and evaluate 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.

  Procedure
  - Maintain, monitor, and evaluate 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.

References
- SOC for Service Organizations - https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations
- Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy with 2022 Revised Points of Focus - https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022
- SOC 2 Frequently Asked Questions - https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/56175896-2011-04977-soc-2-commonly-asked-questions-final.pdf

SOC 2 - Trust Services Criteria A1.1.1 - Measures Current Usage

SOC 2 - Trust Services Criteria	Other Requirements
A1.1.1 Measures Current Usage	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

The use of the system components is measured to establish a baseline for capacity management and to use when evaluating the risk of impaired availability due to capacity constraints.

Guidance
The use of the system components must be measured to establish a baseline for capacity management and to use when evaluating the risk of impaired availability due to capacity constraints. Laws, regulations, contracts, and insurance policies should be reviewed for specific requirements.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- TSC-A1.1.1 - Usage Measurement: Measure the use of the system components to establish a baseline for capacity management and to use when evaluating the risk of impaired availability due to capacity constraints.

  Procedure
  - Measure the use of the system components to establish a baseline for capacity management and to use when evaluating the risk of impaired availability due to capacity constraints.

References

- SOC for Service Organizations - https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations
- Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy with 2022 Revised Points of Focus - https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022
- SOC 2 Frequently Asked Questions - https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/56175896-2011-04977-soc-2-commonly-asked-questions-final.pdf

SOC 2 - Trust Services Criteria A1.1.2 - Forecasts Capacity

SOC 2 - Trust Services Criteria	Other Requirements
A1.1.2 Forecasts Capacity	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

The expected average and peak use of system components is forecasted and compared to system capacity and associated tolerances. Forecasting considers capacity in the event of the failure of system components that constrain capacity.

Guidance
The expected average and peak use of system components is forecasted and compared to system capacity and associated tolerances. Forecasting considers capacity in the event of the failure of system components that constrain capacity.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- TSC-A1.1.2 - Capacity Forecasts: Forecast the expected average and peak use of system components and compared e forecast to system capacity and associated tolerances. Consider capacity in the event of the failure of system components that constrain capacity.

  Procedure
  - Forecast the expected average and peak use of system components and compared e forecast to system capacity and associated tolerances. Consider capacity in the event of the failure of system components that constrain capacity.

References

- SOC for Service Organizations - https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations
- Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy with 2022 Revised Points of Focus - https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022
- SOC 2 Frequently Asked Questions - https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/56175896-2011-04977-soc-2-commonly-asked-questions-final.pdf

SOC 2 - Trust Services Criteria A1.1.3 - Makes Changes Based on Forecasts

SOC 2 - Trust Services Criteria	Other Requirements
A1.1.3 Makes Changes Based on Forecasts	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

The system change management process is initiated when forecasted usage exceeds capacity tolerances.

Guidance
The system change management process must be initiated when forecasted usage exceeds capacity tolerances. Laws, regulations, contracts, and insurance policies should be reviewed for specific requirements.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- TSC-A1.1.3 - Capacity Limits: Initiate the system change management process when forecasted usage exceeds capacity tolerances.

  Procedure
  - Initiate the system change management process when forecasted usage exceeds capacity tolerances.

References
- SOC for Service Organizations - https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations
- Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy with 2022 Revised Points of Focus - https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022
- SOC 2 Frequently Asked Questions - https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/56175896-2011-04977-soc-2-commonly-asked-questions-final.pdf

SOC 2 - Trust Services Criteria A1.2 - Environmental Protections

SOC 2 - Trust Services Criteria	Other Requirements
A1.2 Environmental Protections	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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.

Guidance
The entity must authorize, design, develop or acquire, implement, operate, approve, maintain, and monitor environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. Laws, regulations, contracts, and insurance policies should be reviewed for specific requirements.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- TSC-A1.2 - Environmental Protections: Authorize, design, develop or acquire, implement, operate, approve, maintain, and monitor environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

  Procedure
  - Authorize, design, develop or acquire, implement, operate, approve, maintain, and monitor environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

References
- SOC for Service Organizations - https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations
- Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy with 2022 Revised Points of Focus - https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022
- SOC 2 Frequently Asked Questions - https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/56175896-2011-04977-soc-2-commonly-asked-questions-final.pdf

SOC 2 - Trust Services Criteria A1.2.1 - Identifies Environmental Threats

SOC 2 - Trust Services Criteria	Other Requirements
A1.2.1 Identifies Environmental Threats	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

As part of the risk assessment process, management identifies environmental threats that could impair the availability of the system, including threats resulting from adverse weather, failure of environmental control systems, electrical discharge, fire, and water.

Guidance
As part of the risk assessment process, management must identify environmental threats that could impair the availability of the system, including threats resulting from adverse weather, failure of environmental control systems, electrical discharge, fire, and water. Laws, regulations, contracts, and insurance policies should be reviewed for specific requirements.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- TSC-A1.2.1 - Environmental Threat Identification: As part of the risk assessment process, ensure that management identifies environmental threats that could impair the availability of the system, including threats resulting from adverse weather, failure of environmental control systems, electrical discharge, fire, and water.

  Procedure
  - As part of the risk assessment process, ensure that management identifies environmental threats that could impair the availability of the system, including threats resulting from adverse weather, failure of environmental control systems, electrical discharge, fire, and water.

References
- SOC for Service Organizations - https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations
- Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy with 2022 Revised Points of Focus - https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022
- SOC 2 Frequently Asked Questions - https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/56175896-2011-04977-soc-2-commonly-asked-questions-final.pdf

Truncated Sample Document