[Company name]

System Description

Report	SOC 2 Type 1 or Type 2, Section 3
System	[System name]
As of, or period	[As-of date], or [Period start] to [Period end]
Prepared by	[Company name] management

1. How to use this template

Write in the present tense about what runs today, and name every system, vendor and role. Each part below opens with what belongs in it and the wording a CPA firm sends back. Replace the bracketed prompts, then delete the guidance notes.

2. Services and commitments

> What belongs here: What the service does, who uses it, the commitments you make, and the system requirements behind them. What gets sent back: A sentence about a secure, leading platform. No system in it.

[Company name] provides [System name], [What the service does].

[Company name] designs its processes and procedures for [System name] to meet the commitments it makes to its customers, including:

- [First commitment]
- [Second commitment]
- [Third commitment]

[Company name] also sets system requirements: the specifications the system must meet to deliver those commitments, drawn from its policies, its contracts and the laws that apply to it. They include:

- [First system requirement]
- [Second system requirement]

3. System boundary

> What belongs here: The products and environments inside the examination, and what is outside. What gets sent back: Our production environment and supporting systems. Names nothing, bounds nothing.

The system is [System name] and the infrastructure supporting it, running in [Cloud accounts and regions]. In scope are [Production components]. Access to the application is controlled through [Identity provider] and access to the cloud account through [Cloud access service]. [Items outside the boundary] are outside the boundary. [Company name] operates no data center, so physical controls belong to [Cloud provider] and are carved out.

4. Infrastructure

> What belongs here: Cloud accounts, regions, networks, databases and object storage, by name. What gets sent back: Hosted on a major cloud provider. One vendor is not an inventory.

Component	What it is	Provider and region
Compute	[Cluster, functions or servers that run the application]	[Provider, region]
Database	[Primary database and its replicas]	[Provider, region]
Object storage	[Buckets holding customer files or backups]	[Provider, region]
Network	[Virtual networks, load balancers and firewalls]	[Provider, region]

5. Software

> What belongs here: The application, repositories, build and deploy pipelines, identity, logging, ticketing. What gets sent back: Industry standard tooling. Nobody can request evidence from an unnamed tool.

Purpose	Tool	What it does in the system
Application	[System name]	[What the application does]
Source code and pipelines	[Code repository]	[Code hosting, review and deployment]
Identity	[Identity provider]	[Single sign-on for staff, and how customers sign in]
Logging and monitoring	[Logging system]	[What is logged and alerted on]
Ticketing	[Ticketing system]	[Changes, incidents and access requests]

6. People

> What belongs here: Roles that operate the system, who they report to, who holds production access. What gets sent back: The team follows least privilege, written where a structure belongs.

Role	Reports to	Responsibility	Production access
[Security owner role]	[Role]	Runs the security program	[Yes or no]
[Engineering owner role]	[Role]	Operates production systems	[Yes or no]
[Other role]	[Role]	[Responsibility]	[Yes or no]

7. Procedures

> What belongs here: How change, access, incidents and vendor review actually run. What gets sent back: Policies are documented and maintained. A policy is not a procedure.

Process	How it runs	Governing policy
Access	[How access is requested, approved, reviewed and removed]	Access Control Policy
Change	[How a change is reviewed, tested and deployed]	Change Management Policy
Incidents	[How an incident is declared, handled and reviewed]	Incident Response Plan
Vendors	[How a vendor is assessed before use and reviewed after]	Vendor Management Policy
Backups	[How often backups run and how restores are tested]	Business Continuity and Disaster Recovery Plan

8. Data

> What belongs here: What customer data you hold, how it arrives, where it rests, how long you keep it. What gets sent back: Retention stated as required by law, with no period behind it.

Data	How it arrives	Where it rests	How long it is kept
Customer data	[Upload, integration or API]	[Database and storage, region]	[Contract term, then deleted within a set number of days]
Logs	[Application and infrastructure logs]	[Logging system]	[Log retention period]

Data	How it arrives	Where it rests	How long it is kept
Backups	[Automated snapshots]	[Location separate from production]	[Retention period]

9. System incidents

> What belongs here: Incidents that came from a control failure or significantly failed a commitment: nature, timing, extent and disposition. What gets sent back: No incidents occurred, when the incident log shows one. The log is read.

List each incident, as of [As-of date] for a Type 1 report or during [Period start] to [Period end] for a Type 2 report, that resulted from a control that was not suitably designed or not operating effectively, or that otherwise significantly failed a service commitment or system requirement.

Incident	When	Nature and extent	Disposition
[Incident]	[Date]	[What happened and what it affected]	[How it was resolved and what changed]

If none meets that bar, say so in one sentence: no such system incidents were identified. Your incident log is read against this part.

10. Subservice organizations

> What belongs here: Every vendor the description depends on, named, with your method stated. What gets sent back: A vendor list with no method. Nobody can tell what was tested.

Organization	Service	Method	Controls assumed of it
[Cloud provider]	Hosting and physical security	Carve out	[Physical access, environmental protection, hardware disposal]
[Identity provider]	Authentication	Carve out	[Availability and integrity of the sign-in service]
[Organization]	[Service]	[Carve out or inclusive]	[Controls]

11. Complementary user entity controls

> What belongs here: What the customer must operate for your controls to achieve what you claim. What gets sent back: Customers are responsible for their own security. Names nothing, moves nothing.

Control the customer operates	Owner at the customer	Frequency or trigger
The user entity reviews its administrative users quarterly and removes access when an employee leaves.	[Customer administrator]	Quarterly, and on each departure
[Control the customer must operate]	[Owner]	[Frequency or trigger]

12. Controls and criteria

> What belongs here: Your controls, written the way they run, mapped to the criteria in scope. What gets sent back: A control in the future tense. This section describes what runs.

Control ID	Control, as it runs	Criteria
[AC-01]	[Access to production is approved by a manager before it is granted and reviewed quarterly.]	[CC6.2, CC6.3]
[CM-01]	[Every change is reviewed by someone other than its author before it is deployed.]	[CC8.1]
[Control ID]	[Control]	[Criteria]

13. Criteria not relevant to the system

> What belongs here: Any applicable criterion that does not apply to the system, and the reason for each. What gets sent back: Not applicable, with no reason. An exclusion has to be explained.

Criterion	Why it is not relevant to the system
[Criterion]	[The reason it does not apply to this system]

If every applicable criterion is relevant, say so in one sentence and delete the table.

14. Changes during the period

> What belongs here: Material changes inside a Type 2 window, and when each one happened. What gets sent back: No significant changes, in a period that contains a migration.

Change	Date	Effect on the system or its controls
[Change, for example a database migration]	[Date]	[What changed and how controls covered it]

15. Fields to complete

Replace every bracketed field in this document with your own detail, then delete this section.

Field	What to enter
[Company name]	Your legal company name.
[Security owner role]	The role that runs the security program day to day, for example Chief Technology Officer.
[Identity provider]	The single sign-on directory, for example Google Workspace or Okta.
[Cloud provider]	Where production runs, for example AWS, Google Cloud or Azure.
[Ticketing system]	Where changes and incidents are tracked, for example Jira or Linear.
[Code repository]	Where source code is hosted, for example GitHub or GitLab.
[Logging system]	Where logs are collected and searched.
[Log retention period]	How long logs are kept, for example one year.
[System name]	The product or service the report covers.
[What the service does]	One sentence on what the service does and who uses it.
[First commitment]	A commitment you make to customers, for example an availability target.
[Second commitment]	For example encryption of customer data in transit and at rest.
[Third commitment]	For example access to production limited to named staff.
[First system requirement]	A specification the system must meet, from a contract, a law or your own policy, for example deleting customer data within 30 days of a contract ending.
[Second system requirement]	For example multi-factor authentication for every staff account with production access.

Field	What to enter
[As-of date]	For a Type 1 report, the single date the description speaks about.
[Period start]	For a Type 2 report, the first day of the period.
[Period end]	For a Type 2 report, the last day of the period.
[Cloud accounts and regions]	For example a single AWS account in one region.
[Production components]	The clusters, databases, storage, repositories and pipelines inside the boundary.
[Cloud access service]	How access to the cloud account is controlled, for example AWS Identity and Access Management.
[Items outside the boundary]	What is excluded, for example the marketing site and the laptop fleet.
[Engineering owner role]	The role that owns production systems, for example engineering lead.

Source

Source: free template from www.polaralabs.com/templates/system-description (CC BY 4.0).