PUBLIC SAFETY CLOUD STANDARDS (PSCS)

Vendor Disclosure & Due Diligence Questionnaire

Version 1.2

Prepared for: _____

Vendor Name: _____

Date Submitted: _____

1. Purpose of This Document

The Public Safety Cloud Standards (PSCS) Vendor Disclosure Questionnaire is intended to provide public safety agencies with transparent, structured insight into a vendor's cloud architecture, operational maturity, security posture, and long-term viability.

This document is to be completed by the vendor.

Vendors are expected to provide:

• Direct written responses to each section

• Supporting documentation where requested

• Clear identification of any areas not currently implemented

• Contact information for follow-up clarification

Responses will be reviewed and independently scored by the requesting agency or advisor.

2. Response Instructions

For each section:

1. Provide a written narrative response.
2. Indicate current maturity status.
3. Attach supporting documentation where applicable.
4. Clearly mark any roadmap or future-state items.

Where documentation cannot be shared due to confidentiality, please describe the control in detail.

3. Critical Capability Disclosure

If any of the following are not currently implemented, please indicate clearly:

☐ Defined RTO and RPO

☐ Multi-Availability Zone deployment

☐ Immutable backups

☐ Documented Incident Response Plan

☐ Historical uptime reporting

☐ Shared Responsibility Model documentation

☐ Customer breach notification timeline

If any item above is unchecked, provide explanation below:

4. Corporate Stability & Strategic Viability

Please provide:

• Years in business

• Ownership structure (public/private)

• Number of total public safety customers

• Number of live cloud customers

• Customer retention rate

• Dedicated cloud engineering team structure

• Dedicated SRE function (if applicable)

• 24/7 on-call coverage model

• 5-year product roadmap summary

• Any acquisitions in past 5 years

• Pending litigation that could impact service continuity

Attachments requested:

☐ Financial summary

☐ Organizational chart

☐ Product roadmap overview

☐ Customer references

Vendor Response:

5. Cloud Architecture & Hosting Model

A. Hosting Architecture

• Cloud provider(s) utilized

• Single-tenant or multi-tenant architecture

• Deployment model (containerized, VM-based, serverless)

• Infrastructure-as-Code usage

• Deployment automation strategy

• Blue/Green or Canary deployment strategy

• Rollback capability

Vendor Response:

B. Availability & Resilience

• Published uptime SLA

• Alignment with hosting provider SLA

• Multi-Availability Zone deployment (describe architecture)

• Multi-region capability (if applicable)

• Automatic failover (describe testing frequency)

• Historical uptime reporting availability

• Customer-observable failover demonstration availability

Vendor Response:

C. Scalability

• Auto-scaling capability

• Load testing practices

• Capacity planning methodology

Vendor Response:

6. Security & Compliance

A. Certifications

Indicate current certifications and provide documentation where available:

☐ SOC 2 Type II

☐ CJIS Compliance

☐ ISO 27001

☐ Annual third-party audit

☐ Independent penetration testing

Vendor Response:

B. Data Security

• Encryption at rest

• Encryption in transit

• Key management approach

• Role-based access control

• Multi-factor authentication enforcement

• Backup architecture (including immutability)

Vendor Response:

C. Security Operations

• 24/7 Security Operations Center

• Centralized logging & SIEM

• Documented incident response plan

• Customer breach notification timeline

• Annual tabletop exercises

Vendor Response:

7. Disaster Recovery & Business Continuity

Please provide:

• Defined RTO

• Defined RPO

• Whether RTO/RPO include incident declaration time

• Cross-region replication architecture

• Disaster recovery testing frequency

• Whether production participates in DR testing

• Whether test results are shared with customers

• Backup frequency and retention

• Shared Responsibility Model documentation

• Defined customer responsibilities

Attachments requested:

☐ DR policy

☐ DR test summary

☐ Backup documentation

Vendor Response:

8. Network Connectivity & Agency Dependencies

• Connectivity model (VPN, Direct Connect, other)

• Bandwidth requirements

• Edge device requirements

• Offline operational capability

• Latency tolerance thresholds

• Satellite internet compatibility testing

• Agency-side monitoring requirements

Vendor Response:

9. Data Ownership, Portability & Exit Strategy

• Data ownership terms

• Data export format

• API access availability

• Exit clause summary

• Data return timeline

• Data deletion certification process

• Migration assistance offered

Vendor Response:

10. Integration & Interoperability

• Documented APIs

• Integration with CAD/RMS/Jail/Mobile

• State/NLETS connectivity

• Third-party integration fees

• Integration support included

Vendor Response:

11. Operational Transparency & Observability

• Public status page

• Historical uptime reporting

• SLA tracking methodology

• SLA credit issuance process

• Change management process

• Maintenance communication process

• Application Performance Monitoring tools used

• Infrastructure monitoring tools used

• Synthetic monitoring usage

• Customer-accessible dashboards

Vendor Response:

12. Support & Customer Success

• 24/7 support model

• Defined response SLAs

• Escalation path

• Dedicated account management

• Onboarding process

• Training program

Vendor Response:

13. Financial Model & Cost Transparency

• Pricing model

• Annual escalator terms

• Infrastructure pass-through costs

• Data storage overage costs

• Integration/migration fees

• Minimum term requirements

• SLA enforcement process

Vendor Response:

14. Product Maturity & Engineering Practices

• Release cadence

• Downtime during releases

• DevSecOps practices

• Automated testing

• Feature flags

• Rollback capability

• Customer feedback integration

Vendor Response:

15. Risk Concentration & Dependencies

• Single cloud provider dependency

• Single region deployment risk

• Key personnel concentration risk

• Subcontractor dependencies

• Third-party service dependencies

Vendor Response:

16. Vendor Attestation

I certify that the information provided in this document is accurate to the best of my knowledge and represents current operational capabilities.

Name: _____

Title: _____

Signature: _____

Date: _____