CDPH Cloud Service Provider (CSP) Requirements

(Supplemental to CDT Cloud Provider Requirements)

1.) Service Maturity and Capabilities

a. CSP must have a defined procedural model for IT governance and management such as ITIL, COBIT etc.
b. CSP must have a recognized information security management system such as NIST 800-53, ISO 27000, etc.
c. CSP must have an organizational structure for information security led by senior management (CISO, Security Architect, Compliance Manager)
d. CSP must have Service Terms which provide for State and CDPH confidentiality and data protection requirements
e. CSP must have Service Level Agreements that provide acceptable compensation/credits for unscheduled outages or service interruptions

2.) Security Lifecycle

a. CSP must have controls in place to protect the lifecycle of CDPH information from creation through to deletion
b. CSP must assure CDPH information in digital and physical formats is securely isolated
c. CSP must have back-ups are encrypted and are in a format that meets CDPH requirements
d. CSP must have back-ups tested for restoration capabilities
e. CSP must have data retention schedules that ensure information is sanitized/deleted when no longer required
f. CSP must have data disposal/sanitization procedures that are auditable and disposal certificates are provided (when applicable)

3.) Personnel Security

a. CSP must have appropriate screening and vetting procedures for internal personnel (besides under CDPH contract terms)
b. CSP personnel must be required to undertake mandatory information security awareness (besides under CDPH contract terms)
c. CSP must have processes in place to ensure personnel return assets when they leave or change role (MFA devices, mobile devices that have access to CDPH data, etc.)
d. CSP must have disciplinary processes for information security and privacy violations (besides under CDPH contract terms)

4.) Data Center Physical Security

a. CSP must provide documentation that key data center components such as utilities, air-conditioning, internet connection, etc., are designed to be redundant
b. CSP must provide documentation that physical and environmental security controls are in place, including fire suppression, access control system, CCTV systems, movement sensors, security personnel, alarm systems, etc.

5.) Application and Platform Security

a. CSP must provide documentation that secure system engineering principles are followed within their Software Development Lifecycle (SDLC) processes
b. CSP must provide documentation that host configuration is hardened against vulnerabilities (deploying hardened operating systems, disabling unnecessary services based on secure build images, etc.)
c. CSP must have monitoring and management technologies implemented for all systems
d. CSP must have multi-tenancy mechanisms configured and operational to separate CDPH applications from other customers

e. CSP Web applications must be compliant with security standards (OWASP, etc.)
f. CSP must have a Change Management Process in place to ensure deployment of validated application patches and updates
g. CSP must have a segregated test and development environment to test application patches and updates
h. CSP must have integration with the CDPH SIEM and DLP solutions
i. CSP must have Web Application Firewall (WAF) and/or WAF integration capabilities
j. If using CDPH's namespace for email is a requirement, the CSP's platform must have the capability of sending while meeting DMARC standards for SPF and DKIM, with SPF scoped to CDPH sending hosts only

6.) Access Control

a. CSP must have and use role-based access control and least privilege models
b. CSP's system administrator's access must be reviewed/revoked when personnel change role or leave the CSP's employment
c. CSP must restrict access to any administrative functions of the hosted platform to vendor and/or CDPH assets via source IP restrictions or other methods
d. CSP management platform must support and use MFA enrollment as an enforced policy, and TOTP or FIDO as a protocol for MFA (for all users and administrators)
e. CSP will leverage CDPH's Identity Provider IdP for all user and administrative account access except in the necessary case of "break glass" accounts, with the credentials being held by CDPH
f. CSP must have password polices and rotation for users and programmatic access/secret keys
g. CSP must periodically audit access and remove unused credentials and permissions

7.) Network Security

a. CSP's network connectivity must be adequate in terms of availability, traffic throughput, delays and packet loss
b. CSP must have gateway security measures in place against malware attacks
c. CSP must have operational security measures against network-based attacks (IPS/IDS systems, firewalls, etc.)
d. CSP must have multi-tenancy mechanisms operational to separate CDPH network traffic from other customers network traffic
e. CSP must use secure configurations for all components in their cloud architecture
f. CSP remote administration must be operated via a secure communication channel (SSH, TLS, IPSec, VPN, etc.)
g. CSP must provide integration with CDPH's Cloud Access Security Broker (CASB) platform for threat monitoring, DLP, anomalous activity or conditional access policies
h. CSP must have the ability to implement source IP restrictions

8.) Encryption Security

a. CSP communications must use secure encryption protocols (TLS, etc.)
b. CSP must have encryption controls for CDPH information at rest
c. CSP encryption keys must adequately be protected from unauthorized access
d. CSP must have established encryption key rotation policies to limit the impact of a single compromised key

9.) Technical Vulnerability Management

a. CSP must have notifications about scheduled vulnerability testing that may impact services

b. CSP must have routine penetration tests on cloud service infrastructure, including supporting third party subcontractors
c. CSP must have regular independent information security reviews performed on their organization/infrastructure (including any supporting third party subcontractors)
d. CSP must provide visibility into infrastructure or platform security (internal vulnerability scanning reports, OS patching, OS version levels, A/V, threat protection, IDS/IPS or other related visibility or syslog/SIEM feeds, etc.)
e. CSP must use static application/code security analysis

10.) Incident Management

a. CSP must have 24/7 monitoring of the cloud services and prompt response to suspected and known security incidents
b. CSP must have monitoring and logging of system activity including system operational status and user events
c. CSP must have process in place to notify CDPH in real time about security incidents that impact CDPH services or information
d. CSP must have internal or external forensic capability to support incidents investigation and resolution

11.) Business Continuity and Disaster Recovery

a. CSP must have demonstrable business continuity /disaster recovery processes and plans
b. CSP must have regular business continuity / disaster recovery tests to ensure CDPH information and services can be adequately restored in a timely manner
c. CSP must configure automated data backups and virtual machine snapshots across zones and/or regions, according to recovery time and recovery point objectives

12.) Portability and Interoperability

a. CSP must agree to provide CDPH information in an agreed upon format when the service arrangement ends
b. CSP must have standardized or open interfaces to mutually exchange information between applications

13.) Compliance and Transparency

a. CSP and any subcontractors must be compliant with data protection requirements in applicable Federal, State or CDPH contractual or required security frameworks
b. CDPH must retain legal ownership of information processed or held by the CSP
c. CDPH must have the right to audit and/or monitor that system operations and information processing is being conducted under applicable contract terms
d. CSP must provide details of all locations where customer information will be held or processed (US boundaries, etc.)
e. CSP must provide details of subcontractors involved in contract service delivery
f. CSP must have transparency as to what software will be installed on or for CDPH systems and the security requirements / risks resulting from this
g. CSP must have transparency on governmental intervention or viewing rights, on any legally definable third party rights to view information
h. CSP must provide attestation and architectural documentation clearly showing physical and/or logical separation between CDPH assets and other entities and preventative measures against lateral movement of threats.