CDT prior to purchasing non-CDT Internet Access Services. The Internet Access Policy exemption process is defined on the CGEN Exemption Request webpage at cdt.ca.gov.

ARTIFICIAL INTELLIGENCE INTRODUCTION-4986

Artificial Intelligence (AI) is the development of algorithms and systems that enable machines to perform tasks that typically require human intelligence. It encompasses a broad range of applications and processing, from machine learning, deep learning, automated decision making, generative AI, and natural language processing. As technology advances, AI continues to play a transformative role in shaping how we interact with computers and machines, paving the way for innovative solutions across various industries.

The State's AI policy is intended to create practices that benefit state departments including operational efficiencies, reliability, cost savings, innovation, and sustainability.

The State Administration Manual (SAM) Section 4986 will be used to provide state entities with standards and policies related to the planning, implementation, and use of AI tools and technologies.

Definitions can be found under SAM 4819.2.

Additional resources can be found on the Artificial Intelligence Community website.

Generative Artificial Intelligence (GenAI) Policy Introduction-4986.1

Purpose:

The Generative Artificial Intelligence (GenAI) Policy outlines the requirements for the responsible and secure use of GenAI within the State of California to minimize and mitigate the risks related to use of GenAI. The GenAI Policy aims to ensure efficiency, effectiveness, accessibility, confidentiality, integrity, security and privacy of State data. This Policy applies to all GenAI procured or developed by a state entity.

Scope:

Except as otherwise indicated in the specific chapter, the GenAI Policy applies to all State Entities, employees, contractors, and authorized users who access, use, or manage GenAI within the State.

References:

Executive Order (EO): N-12-23

Government Code (GC): 11000, 11545, 11546, 11546.1(e), 11546.7, 11549.63, 11549.63(g), 11549.64, 11549.65, 11549.65(c), 11549.66

State Administrative Manual (SAM): 4819.2, 4819.35, 4940, 4983.1, 4986.1, 4986.2, 4986.3, 4986.4, 4986.5, 4986.6, 4986.7, 4986.8, 4986.9, 4986.10, 4986.11, 4986.12, 4986.13, 5210, 5335

State Contracting Manual (SCM): SCM, Purchasing Authority Standards, 100.3, 2308

State Information Management Manual (SIMM): 19H, 22, 45, 50, 71A, 71B, 140, 141, 5305-F, 5310-C, 5325-A, 5325-B, 5335-A, 5340-A, 5340-C, 5345-A

California Civil Code:1798.29, 1798.3

National Institute of Standards and Technology (NIST) Artificial Intelligence (AI) Risk Management Framework (RMF); 800-53

Definitions for GenAI-4986.2

1. CDT: California Department of Technology.
2. Executive Branch State Entity: State departments, agencies, boards, and commissions that are under the direct authority of the Governor as described in Government Code § 11546.1(e).
3. Material Impact/Materially Impacts: A significant, substantial effect, whether financial or operational, that is so important that it would reasonably influence a decision-making process.
   a. Work conducted utilizing GenAI materially impacts the functionality of a System when such work could have a significant, substantial effect on the System's data integrity, availability, confidentiality, or security, and failure to perform such work in accordance with the terms and conditions of the contract could potentially cause major disruptions to State business operations resulting in financial, reputational, or other damage to the State. Example: Using GenAI to write source code; using GenAI to perform acceptance testing.
   b. Work conducted utilizing GenAI materially impacts risk to the State when such work could have a significant, substantial effect on the State's operations, finances, security, or reputation, and failure to perform such work in accordance with the terms and conditions of the contract would constitute a high likelihood or impact of financial, reputation, or other damage to the State. Example: Using GenAI to examine Non-Public Data; using GenAI to assist in making decisions that affect public health, safety, or welfare.
   c. Work conducted utilizing GenAI materially impacts contract performance when failure to perform such work in accordance with the terms and conditions of the contract would constitute a material breach of contract. Example: Using GenAI to draft reports or other deliverables without human review.
4. Minimum Viable Products (or MVP): An IT solution that only includes minimum capabilities that is used to validate customer needs and demands prior to developing a more fully featured solution.
5. Proof of Concept (or POC): An effort that tests the functionality of a technology or solution.
6. SAM: State Administrative Manual.
7. SCM: State Contracting Manual.
8. SIMM: State Information Management Manual.
9. State Entity: Executive Branch State Entities as well as any departments, agencies, boards, commissions, colleges and universities, entities headed by constitutional officers or independently established entities described in Government Code § 11000 which are outside the control of the Executive Branch.
10. For all other defined terms used in the GenAI Policy, please see SAM § 4819.2.

References:

GC 11546.1(e); GC 11000; SAM 4819.2

GenAI Use Identification and High-Risk Inventory-4986.3

Scope:

This Chapter of the GenAI Policy applies to all Executive Branch State Entities.

Policy:

Pursuant to this GenAI Policy, the senior management personnel of each Executive Branch State Entity must identify, track, and maintain an inventory of GenAI uses as set forth below.

A. Identify and define the GenAI business need(s), use, risk, and impact through measured analysis of data, systems, environments, projects, privacy, security, and training.

B. Maintain an inventory of high-risk uses of GenAI.

C. Submit the GenAI high-risk system inventory based on the SIMM 5305-F GenAI Risk Assessment criticality to CDT upon request.

References:

EO N-12-23

GenAI Training Data and Transparency-4986.4

Scope:

This Chapter of the GenAI Policy applies to all State Entities.

Policy:

Pursuant to this GenAI Policy, each State Entity must be transparent with respect to the data used to train a GenAI system or service developed by the State Entity as set forth below.

A. On or before January 1, 2026, a State Entity shall post on its internet website documentation regarding the data used to train its GenAI system or service if all the following apply:
   1. On or after January 1, 2022, a State Entity developed GenAI system or a service, or made a substantial modification to GenAI system or service it had released; and
   2. That GenAI system or service is made available to Californians for use, regardless of whether the terms of that use include compensation.

B. The documentation posted by the State Entity must include a high-level summary of the datasets used in the development of the GenAI system or service and include the specific information set forth in Civil Code § 3111.

C. After the initial reporting, the State Entity shall update the documentation on its internet website on an annual basis.

References:

GC 11546.7; Civil Code 3111

GenAI Hosting-4986.5

Scope:

This Chapter of the GenAI Policy applies to all Executive Branch State Entities

Policy:

A. An Executive Branch State Entity considering a new, expansion, or refresh of GenAI must comply with the SAM 4983.1 Cloud Computing Policy, including but not limited to:
   1. Complete the SIMM 140 Cloud Security Guide.
   2. Complete the California Cloud Services Assessment Guide, SIMM 141.
   3. Acquire all Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) solutions and services through the CDT.
   4. Complete a Commercial Off the Shelf (COTS)/SaaS Acquisition Information Form, SIMM 22.
   5. Utilize Software as a Service (SaaS) provided through the CDT state service offerings or through the Department of General Services (DGS) Software Licensing Program (SLP) when implementing GenAI SaaS.

B. An Executive Branch State Entity shall host all software applications at a CDT approved data center.

References:

SAM 4983.1; SIMM 22; SIMM 140; SIMM 141; GC 11546

GenAI Proof of Concept (POC) and Minimum Viable Product (MVP)-4986.6

Scope:

This Chapter of the GenAI Policy applies to all Executive Branch State Entities.

Policy:

A. All GenAI POCs shall be hosted in a CDT approved "sandbox" environment.
   1. POC testing shall not be performed in a production environment.

B. All GenAI MVP shall be hosted in a CDT approved production environment.
   1. All MVPs testing must be performed in a test environment.

C. As part of the POC and MVP, an Executive Branch State Entity must:
   1. Test the feasibility of GenAI to determine if it aligns with the specific needs and objectives of the use case.
   2. Validate the performance, accuracy, and relevance of GenAI by assessing its ability to produce outputs that meet the desired quality and application standards.
   3. Implement risk mitigation strategies to address potential challenges, such as model bias, hallucination, bad actors, equity, and data quality issues, by identifying and addressing these risks during the POC phase.
   4. Limit the data used for testing public data for any POC and ensure that testing for both POCs and MVPs includes any necessary data pre- processing of State-provided data. Data pre-processing should ensure the data is adequately prepared for use with the GenAI solution including scanning for sensitive or classified information (e.g., Personally Identifiable Information (PII), Personal Health Information (PHI), and Federal Tax Information (FTI)). Appropriate measures must be implemented to identify and block such sensitive data.

D. Any GenAI POC that goes into production must be hosted in a CDT approved data center.

References:

EO N-12-23;SAM 4983.1;SIMM 140;SIMM 141

IT Projects Utilizing GenAI Planning and Approval-4986.7

Scope:

This Chapter of the GenAI Policy applies to all Executive Branch State Entities.

Policy:

An Executive Branch State Entity must comply with the following prior to procuring and/or developing an IT project utilizing GenAI.

1. Complete SIMM 5305-F Generative Artificial Intelligence Risk Assessment and SIMM 5310-C Privacy Threshold Assessment and Privacy Impact Assessment as detailed in SAM 4986.9 GenAI Procurement.
2. Comply with SIMM 19H Project Delivery Lifecycle (PDL) for IT projects utilizing GenAI. For clarity, for non-GenAI, an Executive Branch State Entity must complete SIMM 19A-G Project Approval Lifecycle (PAL) policies and comply with the PAL process outlined in SAM 4819.35.

References:

GC 11545; GC 11546; SAM 4819.35; SAM 4986.9; SAM 5210; SIMM 19A-G; SIMM 19H; SIMM 5305-F; SIMM 5310-C

IT Projects Utilizing GenAI Project-4986.8

Scope:

This Chapter of the GenAI Policy applies to all Executive Branch State Entities.

Policy:

A. An Executive Branch State Entity that is approved to proceed with an IT project utilizing GenAI must comply with the applicable parts of SIMM 19H Project Delivery Lifecycle (PDL) for IT projects utilizing GenAI and follow SIMM 45 IT Project Oversight Framework as directed by CDT.

References:

GC 11545, GC 11546, SAM 4819.35; SAM 4940; SIMM 19H; SIMM 45, SIMM 50

GenAI Procurement-4986.9

Scope:

This Chapter of the GenAI Policy applies to all State Entities except as specifically exempted by statute or policy.

A. **Policy:** GenAI Procurement

1. A State Entity shall consider procurement and enterprise use opportunities in which GenAI can improve efficiency, effectiveness, accessibility, and equity of government operations pursuant to CDT's procurement policy.
2. A State Entity must comply with the State Contracting Manual (SCM), Volume 2, Chapter 23, GenAI Procurement Policy and Procedure, when procuring GenAI, as applicable, including but not limited to the mandatory GenAI procurement training.
3. A State Entity must include the following GenAI disclosure notification language in all solicitations and contracts for IT and telecommunication goods and services.

   "Contractor must notify the State in writing if it: (1) intends to provide GenAI as a deliverable to the State; or (2), intends to utilize GenAI, including GenAI from third parties, to complete all or a portion of any deliverable that materially impacts: (i) functionality of a State system, (ii) risk to the State, or (iii) Contract performance. For avoidance of doubt, the term "materially impacts" as used in this section shall have the same meaning set forth in the State Administrative Manual (SAM) § 4986.2 Definitions for GenAI."

4. A State Entity must complete a Certification of Compliance with IT Policies, SIMM 71B.
5. For all IT, non-IT, and Telecommunication procurements, a State Entity must, prior to award, complete a SIMM 5305-F Generative Artificial Intelligence Risk Assessment to determine if the GenAI risk is low, moderate, or high. The State Entity shall submit the completed 5305-F to CDT for all risk levels.
   a. If a State Entity's SIMM 5305-F assessment indicates a moderate or high-risk GenAI, the State Entity shall seek consultation with CDT prior to the award.
   b. If a State Entity's SIMM 5305-F assessment indicates a low-risk GenAI, the State Entity may continue with procurement. For low-risk, CDT may require the State Entity to seek consultation.
   c. The following list of low-risk GenAI uses are exempt from the 5305-F risk assessment requirement:
      1. Mandatory California Prison Industry Authority (CALPIA) purchases of goods and services (See SCM Vol. 2, Chapter 5, Section 502).
      2. Mandatory services provided by Office of State Publishing (OSP).
      3. Mandatory services provided by CDT.
      4. Purchases from DGS Surplus Property.
      5. Real Property Transactions (e.g. leases, easements, rental agreements, licenses, amendments, etc.).
      6. Interagency agreements between CA state departments that do not include third party contracts.
      7. Commodity types that do not include a technology or service component. Examples include:
         a. Office, medical, and cleaning supplies (staplers, pens, masks, mops, etc.)
         b. Office furniture (chairs, desks, etc.)
         c. Non-IT hardware (hammer, nails, buckets, etc.)
      8. Cloud computing software licenses or subscriptions to access online content including news, training, digital publications, etc.
      9. Any other GenAI use determined by CDT to be low risk.
6. For all GenAI procurements, a State Entity must complete a SIMM 5310-C Privacy Threshold Assessment and Privacy Impact Assessment and provide it to CDT for review upon request.
7. A State Entity must have a multidisciplinary governance team to continuously oversee and monitor for new, ongoing, and changing security, privacy, and operational risks throughout the lifecycle of the GenAI use.

A. Contract Security Provisions

For moderate and high risk GenAI use, a State Entity must evaluate vendors and suppliers who provide GenAI for compliance with the SAM 5300, SIMM 5300 and the National Institute of Standards and Technology (NIST) Artificial Intelligence (AI) Risk Management Framework (RMF) and NIST 800-53. Security and Privacy Controls for Information Systems and Organizations for system controls and principles, including security, transparency, and ethical use of data, including but not limited to:

1. Verifying adherence to state policies, privacy laws, and bias mitigation practices.
2. Mandating incident reporting, logs, and cooperation in case of system failures or breaches.
3. Ensuring that vendors and suppliers have robust measures to protect confidential, proprietary, and sensitive data, including encryption, access controls, and compliance with data privacy regulations associated with the state entity's industry.
4. Ensuring that vendors and suppliers provide documentation on the development, training, and operation of their GenAI systems, including details on the origin of datasets, algorithms, and any pre-trained models used.

References:

GC 11549.65(c); Purchasing Authority Standards 100.3; SCM Chapter 23; SIMM 19H; SIMM 71A; SIMM 71B; SIMM 5305-F; SIMM 5310-C

Privacy for GenAI-4986.10

Scope:

This Chapter of the GenAI Policy applies to all State Entities.

Policy:

A. Privacy and Security

1. A State Entity using or procuring GenAI must protect the privacy and security of data in accordance with state and federal laws and policies.
2. A State Entity must implement measures to prevent unauthorized access, use, or sharing of confidential, proprietary, and sensitive state data used by GenAI.

A. Privacy Disclosures

For the transparency of the use of GenAI, irrespective of data classification, all GenAI which involves state data, or provides public service are required to notify consumers that they are interacting with GenAI as described below.

1. All content created or substantially altered by GenAI must have a specified disclosure that the content is generated or substantially altered using GenAI.
2. A State Entity that provides content to a person for government services that was created or substantially altered by GenAI must ensure those communications include:
   i. A disclaimer before the use or consumption of GenAI indicating that the communication type outlined in the Government Code § 11549.66 was generated by GenAI.
      A. A disclaimer example: "This (image/audio/video/text/other form of data) has been generated, in whole or in part, using artificial intelligence."
   ii. A description of how the person may contact an employee of the state entity with appropriate contact information.
3. A provision to opt-out of communicating with GenAI and speak to a real person.
4. A State Entity ingesting data to train GenAI models from external sources, including customers and other systems (including GenAI), must disclose any data that is collected, processed, or shared with trusted partners to the data subject.

References:

Civil Code 1798.29; 1798.3; GC 11549.66

Security for GenAI-4986.11

Scope:

This Chapter of the GenAI Policy applies to all State Entities.

Policy:

A. Security Incident Reporting

1. Violations or incidents involving the use, disclosure, or breach of GenAI and state data must be addressed through a clearly defined reporting and escalation process. This process should be integrated into the State Entity's Incident Response Plan and Playbook, ensuring compliance with the standards outlined in SIMM 5340-A Incident Reporting and Response Instructions and SIMM 5340-C Requirements to Respond to Incidents Involving a Breach of Personal Information.
2. A State Entity must promptly report all suspected or confirmed violations and incidents to oversight agencies.
    a. New identified threats and Tactics, Techniques, and Procedures (TTPs) must be reported to oversight agencies.

B. Security Frameworks

1. A State Entity should leverage the NIST AI Risk Management Framework (AI RMF) to identify, assess, and mitigate risks associated with GenAI, ensuring their development and use align with principles of reliability, fairness, and accountability.
2. A State Entity must document potential risks associated with GenAI throughout their lifecycle, including technical, operational, privacy, legal, ethical, and societal risks in their risk register.
3. A State Entity must ensure that all GenAI adheres to NIST 800-53 Security and Privacy Controls for Information Systems and Organizations to help ensure SIMM and SAM policies are met at a minimum baseline.

C. Security Compliance

1. A State Entity must inventory and document all GenAI systems in a Business Impact Analysis and System Security Plan (SSP) that is submitted with the State Entity's Technology Recovery Plan as outlined in SIMM 5325-A Technology Recovery Plan Instructions and SIMM 5325-B Technology Recovery Program Certification.
    a. All data for GenAI must be classified and documented in their SSPs if applicable.
2. All GenAI (procured or developed by a State Entity) must have an associated SIMM 5305-F Generative Artificial Intelligence Risk Assessment and SIMM 5310-C Privacy Threshold Assessment and Privacy Impact Assessment, unless specifically exempted, as detailed in SAM 4986.9, GenAI Procurement.
3. All GenAI systems must align with SAM 5335 Information Security Monitoring Policy for real time continuous monitoring. Work tools with, GenAI features, are also to align and be monitored in accordance with SAM 5335 when available.
4. A State Entity must continuously oversee and monitor new, ongoing, and changing security, privacy, and operational risks for any GenAI use.
    a. State entity must implement controls and safeguards to mitigate identified risks outlined in SIMM 5345-A Vulnerability Management Standard and ensure compliance with applicable laws, regulations, and ethical standards.
5. A State Entity must approach all GenAI from a Zero Trust Architecture perspective.

References:

SAM 4986.9; SAM 5335; SIMM 5305-F; SIMM 5310-C; SIMM 5325-A; SIMM 5325-B; SIMM 5335-A; SIMM 5340-A; SIMM 5340-C; SIMM 5345-A

Acceptable Use of GenAI-4986.12

Scope:

This Chapter of the GenAI Policy applies to all Executive Branch State Entities.

Policy:

A. An Executive Branch State Entity is responsible for educating and ensuring all users comply with its Acceptable Use Policy and data sharing agreements.

1. GenAI must not be used for, or to create or generate:
    a. Illicit content.
    b. Content that is politically regulated, unlawful material, or information that lacks broad factual verification or consensus.
    c. Spoofs or fraud, including deepfake, impersonation, misinformation, phishing, or social engineering to harm individuals.
    d. Content that may interfere with the principles of Diversity, Equity, Inclusion, and Accessibility (DEIA) of individuals.
2. All GenAI output used for decision making must be supplemented with human verification to ensure accuracy and factuality.
3. All GenAI input and output data must be reviewed to ensure compliance with principles of DEIA and to prevent biases, misuse, and misinformation.

B. An Executive Branch State Entity's Acceptable Use Policy must outline: (1) the risks associated with GenAI, (2) how to use GenAI safely and (3) additional GenAI requirements set forth below.

1. Users only use state approved or provided accounts on state approved or provided equipment for state work.
2. Users are prohibited from entering confidential, proprietary, and sensitive state data into commercially available GenAI.
3. Users may employ GenAI to enhance the efficiency and effectiveness of public services.
4. Users must review and verify GenAI output for relevance before use to ensure it aligns with its intended purpose and to mitigate risks such as hallucinations, misinformation and bias.
5. Users must not infringe on any copyright or intellectual property laws and must comply with open-source licenses as applicable.
6. Users must use the "opt-out" option on data collection and model training features that these GenAI might offer if available. (e.g. ChatGPT).
7. Users waive all rights of ownership to GenAI outputs that are created on behalf of California and used for public related services to California.
8. Users must not use state email or other state identifying information to register unsupported tools.
9. Users must not label content created from GenAI as their own.
10. Users must report the unauthorized use or disclosure of confidential, proprietary, and sensitive state data in GenAI to the Executive Branch State Entity's Information Security Officer (ISO).

References:

EO N-12-23; GC 11546.7; GC 11549.63; GC 11549.64; GC 11549.65; GC 11549.66

GenAI Workforce Training-4986.13

Scope:

This Chapter of the GenAI Policy applies to Executive Branch State Entities.

Policy:

A. Each Executive Branch State Entity must ensure that its personnel complete the necessary GenAI training to perform their duties and responsibilities. This includes understanding the potential risks and benefits of GenAI and how to use them responsibly.

1. State Entities must require employees to complete any mandatory training required for GenAI use.
2. State Entities should also consider the following:
   a. Require all employees to attend foundational GenAI training before deploying GenAI tools.
   b. Require Managers and Supervisors to attend foundational GenAI training and specialized roles training relevant to their area of responsibility.
   c. Require purchasing officials to attend procurement training to understand GenAI purchases, associated risks, and the purchasing process.
   d. Require Project Managers to attend training in the Project Delivery Lifecycle (PDL) for IT projects using GenAI.
   e. Require technology and information security employees to attend advanced GenAI technical training focused on security, data analytics, engineering and development.

References:

EO N-12-23; GC 11549.63 (g); SCM Volume 2, SIMM 19H

DESKTOP AND MOBILE COMPUTING POLICY-4989

The California Department of Technology (Department of Technology) delegates authority to acquire desktop and mobile computing commodities to Agencies/state entities that have submitted acceptable Technology Recovery Plans or Technology Recovery Plan certifications, maintain compliance with all applicable state IT security provisions as defined in SAM Sections 5300-5399, and have appropriate plans for the use of desktop and mobile computing commodities.

Under the Desktop and Mobile Computing Policy, Agencies/state entities are delegated the authority to acquire desktop and mobile computing commodities to support increased staffing, as well as the ongoing replacement of obsolete or nonfunctioning desktop and mobile computing commodities. All acquisitions related to desktop and mobile computing must be consistent with the Agency/state entity's overall strategy for the use of information technology, as expressed in its current Agency Information Management Strategy (AIMS) (See SAM Sections 4900.2 - 4900.6). Agencies/state entities must ensure that the use of mobile computing devices will cost-effectively meet a significant business need and increase the efficiency of the Agency/state entity.

Many desktop and mobile computing commodities are targeted to consumers rather than business users. While these consumer-based commodities are effective as consumer devices, they may not be well-suited for many business uses. To ensure commodities support business productivity and enterprise capabilities, Agency/state entities must understand their security and architecture requirements and acquire the right tools to meet those requirements. Desktop and mobile computing configurations must make use of proven, "off-the-shelf" hardware and software and must support business productivity and enterprise capabilities such as:

- Enterprise Productivity (MS Office)
- Access to Corporate Servers (File/Print, Active Directory, etc.)
- Enterprise Class Applications (Geographic Information Systems, Enterprise Resource Planning, etc.)
- Enterprise Security (VPN, Active Directory Authentication, Multifactor Authentication, etc.)

The acquisition of new mobile computing devices for existing staff should replace existing desktop computers or mobile computing devices, not be purchased in addition to a desktop computer (for example a new laptop should replace a desktop computer). Additionally, the acquisition of new mobile phones should replace desk phones when practical. Replacement of desktop and mobile computing commodities acquired as part of a previously approved IT project, as defined in SAM Section 4819.2, may be included in this policy as such commodities are incorporated into and are no longer distinguishable from the Agency/state entity's IT infrastructure.

DEFINITION OF DESKTOP AND MOBILE COMPUTING-4989.1

Communication – For the purpose of interpreting this policy, communication is the requesting, sending, transmitting, or receiving of electronic data via cable, telephone wire, wireless, or other communication facility.

Desktop and Mobile Computer Software – Commercially licensed software necessary for the operation, use, and/or security of desktop and mobile computers.

Desktop and Mobile Computer Supplies – Consumable commodities used for data storage, printing, and/or other IT supplies as defined in SAM Section 4819.2.

Desktop and Mobile Computing – For the purposes of this policy, desktop and mobile computing is the use of desktop and mobile computing commodities in support of state Agency/state entity business operations.

Desktop and Mobile Computing Commodities – Hardware and software commonly required for most state employees to perform daily business transactions such as desktop computers, mobile computers (e.g., personal digital assistants, laptop computers), mobile phones (e.g. cell phones, smartphones), desktop and mobile computer software, servers, server software, peripheral devices (e.g., printers), supplies, and Local Area Network infrastructure.

Desktop and Mobile Computing Servers – Computer servers necessary for the operation, use, and/or security of desktop and mobile computers.

Desktop and Mobile Server Software – Commercially licensed server software necessary for the operation, use, and/or security of desktop and mobile computers.

Desktop Computers – Computing devices, generally designed to remain in a fixed location, that can connect by cable, telephone wire, wireless transmission, or via any Internet connection to an Agency/state entity's IT infrastructure and/or data systems.

Information Technology Asset Management – The effective tracking and managing of IT assets for an Agency/state entity's program and enterprise IT infrastructure and production systems, including the ability to identify and classify Agency/state entity- owned hardware and software, telecommunications, maintenance costs and expenditures, support requirements (e.g., state staff, vendor support), and the ongoing refresh activities necessary to maintain the Agency/state entity's IT assets.

Information Technology Infrastructure – An Agency/state entity's platform for the delivery of information to support Agency/state entity programs and management. Included in the infrastructure are equipment, software, communications, rules, and vision.

Local Area Network (LAN) – Two or more desktop or mobile computers at the same site connected by cable, telephone wire, wireless or other communication facility providing the ability to communicate or to access shared data storage, printers, or other desktop and mobile computing commodities.

Mobile Computers – Portable-computing devices that can connect by cable, telephone wire, wireless transmission, or via any Internet connection to an Agency/state entity's IT infrastructure and/or data systems. The following devices are considered mobile computers:

Laptop/Notebook – A portable Personal Computer (PC) with a clamshell form factor that combines many desktop computer external components into a single device, such as display, speakers, keyboard, and pointing devices. These devices typically run standard PC operating systems. Laptop/Notebook category includes several variations and form factors which include the following:

-Clamshell - traditional laptop/notebook form factor. All the same attributes/components of a PC, but with the keyboard and monitor attached, and of a size that enables for mobile use.

-Ultrabook - laptops that are thinner with longer battery life and touchscreen, wireless display. The Ultrabook category includes 2-in-1 devices that have the ability to convert their look and feel from a traditional clamshell laptop to a tablet/slate. The conversion can be accomplished by detaching, sliding, folding, twisting, etc.