DIGITAL INFRASTRUCTURE, RATEPAYER AND RESOURCE PROTECTION ACCORD

A Statement of Principles on Data Centers as Critical Technology Infrastructure Enabling Digital Abundance While Protecting the General Ratepayer and Resources

SPONSORING COALITION & POLICY PARTNERS

GOLDWATER INSTITUTE

ABUNDANCE INSTITUTE

PACIFIC LEGAL FOUNDATION

TAXPAYERS PROTECTION ALLIANCE

PREAMBLE

Data centers are the physical foundation of the twenty-first-century economy. They are the layer on which digital services, artificial intelligence, cloud computing, financial services, telemedicine, e-commerce, and remote work are built. Every search query, streamed video, financial transaction, medical record, and AI-generated insight depends on data centers functioning reliably and at scale. This infrastructure deserves the same policy attention that prior generations of legislators gave to roads, bridges, telephone networks, and broadband — the foundational infrastructure that enabled broad economic participation and national competitiveness.

The United States currently leads the world in data center capacity, and that leadership is an economic and strategic asset. Maintaining it requires a policy framework rooted in free markets, limited government, federalism, individual liberty, and a pro-growth, abundance mindset. The default policy posture must be one that enables this infrastructure to grow. Outright bans or moratoria on data center development are inconsistent with the recognition of data centers as critical technology infrastructure and are contrary to the principles of this statement.

At the same time, sound policy must ensure that the enormous electric load created by large data centers is not financed on the backs of residential, commercial, agricultural, and industrial ratepayers. A genuinely pro-abundance framework pairs a welcoming environment for private investment with clear rules ensuring that those who cause costs bear them. These principles are offered to guide legislators, regulators, and community leaders toward both objectives.

I. DATA CENTERS ARE CRITICAL TECHNOLOGY INFRASTRUCTURE

Data centers are critical technology infrastructure. The capacity, speed, and reliability of a state's digital footprint directly affect its ability to attract technology investment, support innovation, and enable businesses of all sizes — particularly small businesses, startups, and rural enterprises — to compete on equal footing with larger firms.

Data centers support an ecosystem of economic activity: the companies that build and operate them, the businesses that depend on the cloud and AI services they enable, and the communities that benefit from the employment, tax base, and supply-chain activity they generate.

- **Rejecting Arbitrary Ban:** Outright bans, emergency moratoria, or discriminatory prohibitions on data center development are inconsistent with the recognition of data centers as critical infrastructure. Such restrictions raise the cost and complexity of development, shift vital investment to other regions, and harms American technological leadership and national security.

- **Nuisance Law as the Proper Remedy:** Land-use conflicts regarding noise, lighting, and localized impacts should be handled through well-developed, objective local nuisance law, which provides the appropriate avenue for mitigation. Local concerns should not be weaponized as a pretext for regulatory paralysis or political exclusion.

II. AI AND THE DIGITAL ECONOMY DEPEND ON DATA CENTER INFRASTRUCTURE

Artificial intelligence — including large language models, machine learning systems, and AI-powered applications across healthcare, agriculture, manufacturing, finance, and public services — is computationally intensive. Its development and deployment require growing data center capacity. Decisions that constrain or delay domestic data center development have consequences that extend well beyond the facilities themselves, affecting American competitiveness and the pace at which AI tools become available, affordable, and accessible. Other nations are actively investing in data center capacity and competing to host the future infrastructure of the AI economy; state and federal policies that increase cost, complexity, or uncertainty will shift that investment abroad.

III. PROPERTY RIGHTS, PREDICTABILITY, AND MINISTERIAL APPROVAL

The right to own property includes the right to develop that property for productive use. Data centers represent the modern evolution of commercial infrastructure and should be afforded the same legal certainties as traditional commerce. Transparency and predictability in the policy environment are vital, because developers of data center infrastructure, like all developers of commercial and industrial infrastructure, make long-term capital commitments, and shifting requirements raise costs and drive investment elsewhere.

- **Classification and Consistency:** Data centers should be classified and treated consistently with comparable industrial or commercial uses, governed by objective standards rather than retroactive zoning changes or discriminatory permitting imposed in response to transient political pressure.

- **Vested Rights and Takings Protections:** Once a developer has committed capital and submitted a site plan, development rights should be considered vested, locking in the regulatory and land-use rules in place at the time of filing. States should adopt protections requiring compensation where new regulations cause a significant diminution of property value.

- **Permit by Rule and Shot-Clocks:** Regulatory frameworks designed for traditional industrial facilities are poorly suited to the digital economy. States should favor Permit-by-Rule frameworks, under which approval is a ministerial act granted automatically when a project certifies compliance with objective, pre-established standards, and should adopt mandatory shot-clock provisions so that completed applications are deemed approved by operation of law if a governing body fails to act within a fixed window. These streamlined permitting protections should apply broadly across commercial and industrial sectors to ensure equal regulatory treatment and foster competitive enterprise.

- **Data Security and Privacy:** Transparency requirements must not become instruments of delay or regulatory leverage. State governments must not use land-use approvals, zoning variances, or utility permitting as leverage to extract access to private data, metadata, or proprietary server architecture. Fourth Amendment protections, and the matching state constitutional protections, extend fully to data stored within physical infrastructure, regardless of its physical location within a jurisdiction.

IV. ENERGY ABUNDANCE AND MARKET ACCESS

Artificial intelligence and the broader digital economy require substantial and growing energy capacity. Sustaining this growth requires a framework of energy abundance that empowers consumer choice, protects the property rights of generators and transmitters, and allows market forces to shape the energy landscape.

- **Self-Generation and Co-Location:** Data Centers should have clear authority to secure power — by generating it on-site, contracting for dedicated supply, or integrating co-located systems such as small modular reactors, advanced geothermal, and microgrids — subject only to objective safety and interconnection standards.

- **Technology Neutrality:** Policy for power and water should remain technology-neutral, focusing on objective outcomes rather than mandating specific energy profiles or cooling technologies, which risks locking in practices that do not evolve with technology or local conditions.

- **Direct Market Access:** Data centers interested in contracting for off-site power should have direct market access to negotiate, contract, and purchase power directly from suppliers.

V. FISCAL INTEGRITY AND PROTECTION OF THE GENERAL RATEPAYER

Infrastructure expansion must not socialize the costs of large-scale industrial demand. Data centers can and should function as a net fiscal contributor to the communities that host them — but only under rules that ensure the costs of serving extraordinary new electric load are borne by those who cause them, not shifted onto households and existing businesses. A beneficiary-pays model is both sound free-market policy and the surest way to maintain public trust in continued data center growth.

- **Cost Causation as the Governing Standard:** Under the public utility regulator model, rates are determined by assigning costs and revenues among customers in accordance with cost-causation principles. Residential, commercial, agricultural, and industrial customers should be protected from paying higher rates resulting directly from electric service to very large new loads.

- **Large-Load Frameworks:** Legislators should codify clear large-load frameworks that protect the general rate base while allowing private developers to scale infrastructure rapidly at their own expense, funding the specific system expansions and transmission upgrades their load requires.

- **Competitive Neutrality:** True competitiveness arises from a low-tax, light-touch environment applied to all innovators equally. Data Centers should enjoy no more than equal sales and use tax treatment as a state applies to all business machinery and equipment. The state should prioritize permanent regulatory certainty over temporary, targeted incentives that pick winners and losers.

- **Role of Public Utility Regulators:** Public utility regulators can require electric suppliers to establish and maintain separate terms, conditions, and tariffs for large load customers, including credit requirements and other measures ensuring that such customers reimburse the supplier for all costs fairly allocated to them — including costs incurred to serve the customer directly that may otherwise go unrecovered if the customer departs the system or materially reduces load.

- **Apply broadly across suppliers:** Apply ratepayer protections to all retail electric suppliers — investor-owned utilities, electric cooperatives, municipal electric utilities, and public power utilities — and vest enforcement in the appropriate regulatory authority, such as the state corporation or public utility commission.

VI. WATER STEWARDSHIP THROUGH EVIDENCE-BASED PERMITTING

Responsible water use is fully compatible with data center growth, and sound policy achieves it without resorting to rigid technology mandates. Permit applicants can be required to demonstrate no harm to the watershed or to neighboring wells before a permit is issued. Existing state and federal permitting processes already provide environmental review for large facilities, and these frameworks can be strengthened where appropriate without displacing the regulatory judgment they were designed to exercise.

- **Project-Specific Evaluation Over Uniform Mandates:** Targeted permitting approaches protect water resources while preserving regulators' flexibility to evaluate each project on its merits — accounting for local recharge rates, existing allocations, and the actual water consumption profile of the proposed facility. A one-size-fits-all technology mandate is the wrong instrument: it may be unnecessary in water-rich regions and inadequate in the most stressed areas.

- **A Performance-Based Safe Harbor:** Rather than dictating engineering methods, states should offer applicants an optional, outcome-based pathway to demonstrate water stewardship. A facility should be deemed compliant — regardless of the cooling technology it employs — where it attests that its cooling system, including both primary cooling circuits and heat rejection systems, achieves a designated water-use effectiveness (WUE) in terms of liters per kilowatt-hour; and that it sources non-potable water to the maximum extent practicable. Facilities operating entirely on reclaimed water should be exempt from the WUE and capacity thresholds altogether. Because these are objective, technology-neutral outcomes, any architecture that meets them qualifies — and applicants remain free to demonstrate no harm by other means where local conditions warrant.

- **Avoid Freezing Technology in Statute:** A uniform mandate risks locking specific engineering standards into law, limiting regulators' ability to adapt permitting decisions as cooling technologies and hydrogeological understanding evolve. The legislature should not be in the business of selecting specific engineering solutions for industrial facilities; that determination is better made by the appropriate regulatory authority on a region-by-region, project-by-project basis.

VII. THE RIGHT TO INNOVATE / RIGHT TO CLOUD COMPUTE

The rapid evolution of artificial intelligence and high-performance computing calls for a regulatory posture that favors experimentation over prohibition. Policy frameworks should be flexible enough to accommodate technological change rather than locking in static assumptions about how data centers operate today. Legislators should reject restrictions grounded in speculative or unproven risks, adopt light-touch frameworks that address tangible, proven harms, and establish regulatory sandboxes that support the iterative, dynamic nature of innovation.

CONCLUSION

Taken together, these principles define a framework that protects individual rights, rewards private initiative, protects the general ratepayer, and ensures that technological growth is driven by free markets rather than bureaucratic mandates. The decisions states make today about the infrastructure of the digital economy will shape their economic position for a generation. We urge legislators to approach data center policy with the same strategic clarity that prior generations of private investment provided for telecommunications and broadband — enabling abundance while maintaining support of the households and businesses that share the grid.