GovTech Innovators

GovTech Innovators, Inc.

AI Policy and Security Considerations in Parks

www.govtechinnovators.com

AI Policy and Security Considerations

AI Tools Used in Parks and Recreation

GovTech Innovators

Common AI Tools for General Use

- Traditional Leading AI Tools: **ChatGPT**, Claude, Google Gemini
- Cove.AI
- InVideo.io, Lumen5, Synthesia, Colossyan (tailored for workplace training videos)
- Google Notebook LM

Common AI Integrations into existing tools

- Canva and Adobe Express have AI integrated for things like generation and editing of images, logos, text, templates, even basic videos.
- Tools like HubSpot have AI integrated for writing marketing emails, generating calls to action, writing catchy subject lines, summarizing information, etc.
- Microsoft Office has implemented AI into their offerings as well with things like the Designer to suggest various formats for your content.
- Approximately 60% of new software products released in 2025 will have AI integrated in some manner, whether it's to summarize text, generate content, analyze large data sets, conduct research, etc.

AI Policy and Security Considerations

Introduction to AI Use Policies

AI Use Policy Defined

- An AI Use Policy is a set of guidelines and regulations established by an organization to govern the development, deployment, and use of artificial intelligence systems.

Benefits of an AI Use Policy

- **Risk Mitigation:** Helps identify and address potential risks associated with AI use, such as bias, privacy breaches, or unintended consequences.
- **Ethical Alignment:** Ensures AI systems are developed and used in accordance with the department's values and ethical standards.
- **Regulatory Compliance:** Aids in meeting legal and regulatory requirements related to AI, data protection, and privacy.
- **Consistency and Standardization:** Provides a framework for consistent decision-making and implementation across the organization.
- **Transparency and Trust:** Demonstrates commitment to responsible AI use, building trust with stakeholders and customers.
- **Innovation and Exploration Guidance:** Encourages innovation within defined boundaries, balancing progress with responsible practices.

AI Policy and Security Considerations

GovTech Innovators

Components of an AI Use Policy

- Purpose and Scope
- Guiding Principles
- Definitions
- Data Governance
- Permitted and Prohibited Uses
- Transparency
- Bias Mitigation
- Risks and Mitigation
- Compliance
- Human Oversight
- Security Protocols
- Training and Awareness
- Incident Response
- Monitoring

AI Policy and Security Considerations

Exploring AI Use Policies

Purpose and Scope

- Defines the intent of the AI use policy, providing a clear understanding of why the policy is being implemented.
- Outlines the specific areas of the department and activities that the policy applies to (e.g., using AI tools like ChatGPT for resident inquiries).

Guiding Principles

- Outlines ethical standards like fairness, accountability, and transparency that guide AI implementation.
- Ensures all AI initiatives are aligned with community values, such as inclusiveness and equity.
- Highlight the importance of resident trust and sets guidelines to avoid AI misuse or unethical behavior.
- Emphasizes responsible AI usage, meaning that AI should assist—not replace—human judgment in decision-making.
- **Example:** AI-driven decisions should always be validated by human staff to maintain accountability and fairness.

AI Policy and Security Considerations

Exploring AI Use Policies

GovTech Innovators

Definitions

- Clarifies key AI-related terms such as "machine learning," "bias," and "personal data" to ensure consistent understanding among all stakeholders.
- Prevents misinterpretations by providing precise definitions, particularly for technical terms used in the policy.
- Helps bridge the knowledge gap for non-technical staff by simplifying AI concepts.

Data Governance

- Provides guidelines on how data will be collected, used, stored, and protected when interacting with AI systems.
- Establishes data privacy measures to ensure compliance with relevant laws, such as not entering PII into AI tools.
- Defines data access protocols—who can access what data and under what circumstances.
- Outlines data retention policies to ensure data used in AI tools is stored only for as long as necessary.

AI Policy and Security Considerations

Exploring AI Use Policies

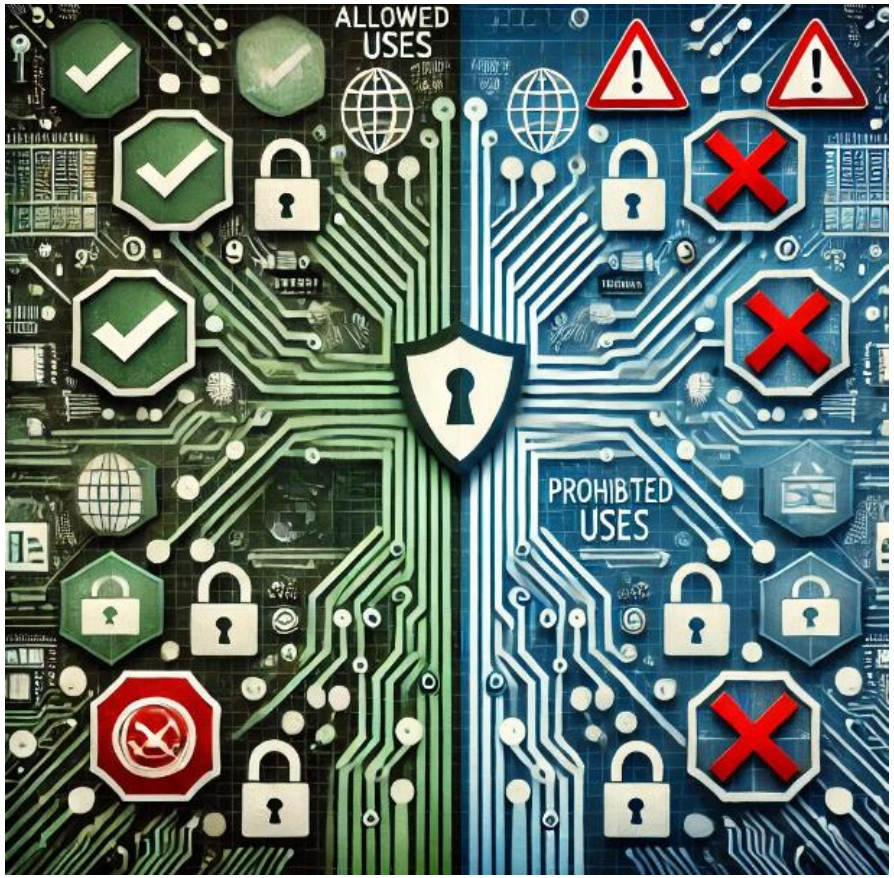
GovTech Innovators

Permitted and Prohibited Uses

- Specifies acceptable use cases for AI, such as drafting promotional content, creating schedules, and responding to general resident inquiries.
- Lists prohibited use cases to prevent misuse, such as using AI to process sensitive personal information or make policy decisions autonomously.
- Ensures that your team knows to use AI tools and when human intervention is required.
- Prevents AI misuse by setting clear boundaries on how tools like ChatGPT should be applied.
- **Example:** AI can be used to augment the generation of newsletter content, but it cannot be used to approve resident applications or permits.

Transparency

- Ensures that AI use, including its purpose, data sources, and limitations, is openly communicated to staff and residents.
- Requires documentation of AI processes, so staff understand how decisions are made and can explain outcomes to residents.
- Promotes trust by providing visibility into how AI tools work and the reasoning behind decisions.
- Highlights the need for residents to be informed when interacting with AI-driven responses, ensuring they know when they're communicating with an AI versus a human.
- **Example:** Adding a disclaimer to AI-generated emails



AI Policy and Security Considerations

Exploring AI Use Policies

Bias Mitigation

- Outlines strategies to identify, monitor, and minimize bias within AI systems, such as regular audits of AI outputs.
- Requires diverse datasets to train AI tools to avoid reinforcing existing biases and to ensure fairness.
- Establishes protocols for addressing biases if found, including escalation and retraining of models where necessary.
- Encourages regular review of AI outputs to identify any potential biases that may affect decision-making.
- **Example:** Testing AI responses for bias when generating promotional content

Risks and Mitigation

- Identifies potential risks such as data privacy issues, ethical concerns, or incorrect AI outputs.
- Requires risk assessments to determine the impact and likelihood of risks associated with AI use.
- Outlines mitigation strategies like limiting the use of AI for high-stakes decisions and ensuring human oversight.
- Encourages proactive identification of risks before AI implementation, rather than reacting to issues after they occur.
- **Example:** Ensuring human oversight for every single AI-generated response to resident communications

AI Policy and Security Considerations

Exploring AI Use Policies

GovTech Innovators

Compliance

- Ensures adherence to relevant laws and regulations governing data privacy, ethical AI use, and accessibility.
- Regularly review AI policies for compliance with evolving legal requirements.
- Establish accountability to demonstrate that AI practices meet all necessary regulatory standards.
- **Example:** Regularly auditing AI data handling practices to ensure adherence to federal and state privacy laws.

Human Oversight

- Establishes roles for humans to supervise AI systems, ensuring that outputs are appropriate and aligned with departmental goals.
- Requires human validation of AI-generated decisions, particularly those that directly impact residents.
- Ensures human intervention is available to override AI in case of errors or inappropriate suggestions.
- Provides guidelines for staff to manage AI systems effectively and understand when escalation to human oversight is necessary.
- **Example:** AI-generated responses to resident emails must be reviewed and approved by department staff before implementation.

AI Policy and Security Considerations

Exploring AI Use Policies

GovTech Innovators

Security Protocols

- Vendor Security Certifications and Compliance: Ensure that AI service providers follow industry-standard security protocols such as encryption, regular patching, and compliance with relevant regulations (e.g., GDPR, CCPA). Confirm that these standards are maintained through contractual agreements and audits.
- Internal Access Control: Implement and manage user-level access within the organization, using features provided by the service provider such as role-based access control and multi-factor authentication (MFA) to limit who can access and manipulate AI systems.
- Service Provider Audits: Regularly review security reports and certifications from AI vendors to ensure they maintain proper security protocols like system monitoring and threat detection, while also conducting internal checks on how the AI systems are integrated and used.

Training and Awareness

- Mandates training programs to educate staff on responsible and knowledgeable use of AI tools.
- Focuses on understanding AI capabilities, limitations, and best practices for using AI tools in daily operations.
- Encourages regular refresher courses to keep staff updated on the latest AI features and potential risks.
- **Example:** Conducting quarterly training sessions to help staff understand updates to AI tools like ChatGPT and their implications for the department.

AI Policy and Security Considerations

Exploring AI Use Policies

GovTech Innovators

Incident Response

- Provides protocols for managing incidents involving AI systems, such as data breaches or incorrect AI outputs.
- Requires clear reporting procedures for staff to follow if an AI-related issue occurs.
- Establishes roles and responsibilities for responding to incidents, ensuring a coordinated response.
- Ensures timely corrective actions to mitigate the impact of AI-related incidents on residents or services.
- **Example:** Designating a team to handle incidents where AI-generated content leads to misinformation or inappropriate communication.

Monitoring

- Establishes ongoing processes to evaluate AI performance and its impact on departmental goals and community services.
- Requires regular reviews of AI tools to identify any performance issues or unintended consequences.
- Sets metrics and KPIs to measure the effectiveness of AI tools in meeting their intended purposes.
- Encourages continuous improvement based on monitoring outcomes, ensuring AI remains valuable to the department.
- **Example:** Monitoring response times and resident feedback to assess the efficiency of ChatGPT in handling resident inquiries.

AI Policy and Security Considerations

DIY Policy vs Hiring Out

Drafting Your Own AI Use Policy

- **Existing Process and Expertise:** Have an existing process and expertise for managing an AI use policy? DIY may be your best option.
- **Time-Consuming:** Developing an AI use policy in-house can be a lengthy process, requiring research into regulations, best practices, and stakeholder needs.
- **Expertise Requirements:** Requires a deep understanding of AI, data privacy, and legal standards to ensure a comprehensive policy.
- **Maintenance Burden:** Regular updates are needed to keep the policy current with new AI trends and changing regulations, which can add an ongoing workload.
- **Example**: A Parks and Recreation department might draft their own AI policy to reflect specific needs, but face challenges in staying up-to-date on evolving technology and compliance requirements.
- **Cost Efficient:** When budgets are tight, every dollar matters

Outsourcing AI Use Policy Creation

- **Tailored Customization:** Policies are customized to meet the specific needs of each department.
- **Expert Guidance:** Gain access to specialists in AI governance who understand the specific needs of Parks and Recreation
- **Efficiency:** Saves time and resources by leveraging an existing framework that can be quickly tailored to your needs.
- **Ongoing Updates:** Policies are maintained and updated regularly to keep up with emerging trends, regulations, and new AI capabilities, reducing the burden on department staff.
- **Example:** Outsourcing the AI use policy to a specialist ensures that the policy remains compliant with evolving regulations, while still reflecting the department's operational goals and community standards.

AI Policy and Security Considerations

Exploring AI Use Policies

GovTech Innovators

Summary and Key Objectives

- The AI use policy establishes a clear framework to guide responsible AI use, focusing on defining the scope, ethical principles, data governance, compliance, and human oversight.
- **Key Objective 1**: Ensure the ethical and transparent use of AI tools within the Parks and Recreation Department.
- **Key Objective 2:** Mitigate risks associated with bias, data privacy, and misuse through clear guidelines and human involvement.
- **Key Objective 3:** Foster a responsible and informed culture around AI use, ensuring staff have the necessary training and oversight measures.

Next Steps

- Evaluate your fit for drafting your own AI Use Policy vs hiring it out and get started, the hardest part is getting started!
- Let's explore ***AI Security Risks!***

AI Policy and Security Considerations

AI Security Risks

AI Security Risks Summarized

- **Data Privacy and Security:** Risks related to unauthorized access, use, or exposure of sensitive data handled by AI systems.
- **Cyber-Attacks:** Vulnerabilities in AI systems that can be exploited by attackers to compromise security or operations.
- **Misuse/Overreliance:** The risk of users making poor decisions by blindly trusting AI outputs without proper human judgment.
- **Bias and Discrimination:** The risk that AI models perpetuate or amplify biases present in training data, leading to unfair outcomes.
- **Ethical and Social Impacts:** Potential unintended negative consequences on individuals or society from AI-driven decisions.
- **Compliance and Legal Risks:** Risks associated with failing to meet regulatory or legal requirements for AI usage.
- **Transparency and Accountability:** Challenges in explaining AI decision-making processes and ensuring responsible parties are held accountable.
- **Human-AI Interaction Issues:** Difficulties users face in understanding, trusting, or appropriately using AI outputs in decision-making.

AI Policy and Security Considerations

Data-Related Risks

Data Privacy and Security

- **Personal Information Sharing:** Staff might inadvertently share personal or sensitive data, such as resident names, addresses, or financial information, without knowing how securely the AI tool handles it.
- **Data Retention:** Data entered in AI systems may be stored and potentially accessed by third parties, raising privacy concerns. For example, data entered into ChatGPT could be retained by OpenAI and potentially used for model improvement or accessed in the event of a data breach.
- **Example:** A staff member might use ChatGPT to draft a response to a resident inquiry and include sensitive details like a resident's address or account information, which could be stored by the AI tool and potentially accessed by unauthorized entities.

Cyber-Attacks

- AI tools, particularly cloud-based ones, can be targets for cyber-attacks, potentially exposing sensitive departmental data.
- Risk of Hacking: If the AI tool or its provider experiences a data breach, information input by staff could be compromised. For instance, if ChatGPT's servers are breached, any data that was input by users could be exposed to attackers, leading to potential misuse of that information.

AI Policy and Security Considerations

Data-Related Risk Mitigation

Risk Mitigation Strategy

- Use a paid version of ChatGPT, either the Teams plan or the Enterprise plan. Plus uses your data unless you opt out.
- Enhanced security features such as end-to-end encryption, data residency options, and stricter data handling policies.
- Your data is not used to retrain models, providing additional privacy and reducing the likelihood of data exposure.
- Establish strict guidelines for staff on what type of information can and cannot be shared with the AI.
- Implement data privacy training to ensure all staff understand the potential risks of sharing personal or sensitive data with AI tools

To Share or Not to Share?

- **To Share:** Drafting promotional material for community events, generating ideas for recreational programs, creating announcements, etc.
- **Not To Share:** Personally identifiable information (PII) like resident names, addresses, or contact information, financial details such as credit card information, health-related information governed by HIPAA.
- **Example:** Using ChatGPT to write a welcome email for new program participants without including any names is appropriate, while asking ChatGPT to review specific resident account details is not.

Cyber-Attacks

- Use AI tools/subscriptions that provide data encryption both in transit and at rest (such as ChatGPT Teams or Enterprise plans)
- Utilize multi-factor authentication for accessing AI tools to add an extra layer of security.
- Regularly review and update security protocols to ensure data safety.

AI Policy and Security Considerations

User Behavior and Interaction Risks

Misuse/Overreliance

- **Risk of Inaccurate Information:** ChatGPT will sometimes generate incorrect or misleading information, leading to poor decision-making or communication with residents. For example, if a staff member uses ChatGPT to answer a resident's question about facility availability, and the AI provides outdated or incorrect information, it could lead to confusion and dissatisfaction.
- **Reduced Human Judgment:** Overreliance on AI can result in staff neglecting to apply their own expertise or judgment. This could be particularly problematic in situations that require nuanced understanding or local context that AI might not be able to fully grasp.

Human-AI Interaction Issues

- **Lack of Understanding:** Users may not fully understand what the AI can and cannot do, leading to unrealistic expectations about its capabilities. For instance, they might expect ChatGPT to provide real-time data or have specific knowledge about internal policies that it was never trained on.
- **Trust Issues:** A lack of transparency in how the AI generates responses can cause staff to either mistrust the tool or place too much trust in it. This can lead to inconsistency in how the tool is used, with some staff avoiding it altogether while others use it inappropriately without verification.

AI Policy and Security Considerations

User Behavior and Interaction Risk Mitigation

GovTech Innovators

Misuse/Overreliance

- Implement training programs that emphasize the limitations just as much as the capabilities of AI tools like ChatGPT.
- Train staff to use AI outputs as starting points rather than definitive answers.
- Establish a process for human review and validation of AI-generated content, especially for public communications or critical information.
- Use built-in tools to flag sensitive or critical responses for further evaluation.

Human-AI Interaction Issues

- Provide clear and concise training for staff on how ChatGPT works, including its capabilities and limitations.
- Adopt processes that require AI-generated content is reviewed before sharing it publicly.
- Encourage staff to use AI as a support tool rather than relying on it entirely for decision-making.
- Consider providing easy-to-understand documentation or FAQs to assist staff in understanding appropriate use cases for the AI.

AI Policy and Security Considerations

Ethical and Bias Risks

Bias and Discrimination

- **Unintentional Bias:** ChatGPT may produce biased responses based on patterns learned from training data, which could negatively impact interactions with diverse community members.
- **Bias Example:** If staff use ChatGPT to generate content related to community events, the tool may inadvertently exclude certain groups or use language that is not inclusive.
- **Impact on Decision-Making:** Biased outputs can influence decision-making processes in ways that reinforce stereotypes or disadvantage specific groups. This is particularly concerning in public services where equitable treatment of all residents is crucial.

Ethical and Social Considerations

- **Impersonal Interactions:** Reliance on AI for resident communication may lead to a perception of reduced empathy or personalization in services. For instance, if residents receive generic AI-generated responses rather than personalized assistance, they may feel undervalued or neglected.
- **Equity Concerns:** Some community members may have less access or comfort with AI-driven interactions, leading to inequities in service delivery. This could result in certain groups being left behind or underserved, particularly if they lack digital literacy or access to technology.

AI Policy and Security Considerations

Ethical and Bias Risk Mitigation

Bias and Discrimination

- Regularly test ChatGPT's outputs to ensure they are unbiased and inclusive, using diverse scenarios that reflect the community.
- If biases are detected, document and report them to the AI vendor for improvements.
- Establish clear guidelines for recognizing and mitigating biased responses.
- Provide staff training to help identify biased outputs from AI.
- Encourage the inclusion of diverse voices and perspectives in your preferences. In ChatGPT you can tell GPT what you want it to know about you and specify response preferences.

Ethical and Social Considerations

- Balance the use of AI tools with personal, empathetic communication when interacting with residents.
- Set clear expectations for when staff should use AI tools and when human interaction is preferable, particularly for sensitive or emotionally charged topics. This starts with your AI Use Policy.
- Gather feedback from residents about their experiences with AI-driven interactions to identify areas of improvement and to ensure equitable service delivery across all demographics.

AI Policy and Security Considerations

Governance and Compliance Risks

Compliance and Legal Risks

- **Data Handling Compliance:** AI tools must comply with federal laws such as the Health Insurance Portability and Accountability Act (HIPAA) if they handle healthcare data, and the Children's Online Privacy Protection Act (COPPA) if any user data involves minors.
- **Example:** Your team use ChatGPT to handle information related to residents' health or minors without proper safeguards, this could result in non-compliance risks.

Transparency and Accountability

- **Opaque Decision-Making:** AI-generated responses can be difficult to explain, which can be problematic in justifying decisions to stakeholders.
- **Example:** If a resident questions a response generated by ChatGPT, staff may struggle to provide a clear explanation since ChatGPT's responses are based on patterns in training data rather than specific, traceable logic.
- **Accountability Gaps:** Without clear understanding, it is hard to determine responsibility if an AI-generated response causes an issue.
- **Example:** if a misleading response from ChatGPT results in misinformation being communicated to residents, it may be challenging to determine whether the staff member, the AI provider, or the department is ultimately responsible, leading to potential accountability issues and disputes.

AI Policy and Security Considerations

Governance and Compliance Risk Mitigation

GovTech Innovators

Compliance and Legal Risks

- Ensure compliance with federal and state laws by working with legal counsel to review policies regarding the use of AI tools like ChatGPT in public services.
- For privacy laws such as HIPAA and COPPA implement appropriate safeguards, and do not enter sensitive information into AI systems, period.
- Ensure compliance with local laws such as the Missouri Data Breach Notification Law and the Kansas Consumer Protection Act.

Transparency and Accountability

- Maintain chat logs using the tool's native features, such as those available in the paid versions of GPT and Claude, so that you have an audit trail that can be reviewed if questions arise.
- Provide a clear accountability structure that assigns responsibility to individuals or teams for reviewing and approving AI-generated content before it is shared with residents.
- Where possible, use AI systems that provide explanations for their outputs to improve transparency and understanding among staff and residents.

Questions?

AI Policy and Security Considerations

Analyze Existing Policies and Identify Gaps

GovTech Innovators

Start with what you have

- Start by assessing your current policy for application to the use of Artificial Intelligence in your Department

Assess Current Policy Landscape

- **Conduct a thorough review of all existing policies:** Technology Use Policies, Data and Privacy, Ethical Guidelines, Risk Management and Security
- **Evaluate Policy Comprehensiveness and Relevance:** Assess if current policies are up-to-date with current technology practices and if they address emerging technologies, including AI.
- **Identify Potential Gaps Related to AI Use:** Document gaps such as data governance for AI-processed information, ethical considerations specific to AI decision-making, and security protocols for AI systems.
- **Holistic Assessment:** Use this documentation to make a holistic assessment of whether it makes more sense to develop a completely new AI Use Policy or to integrate these considerations into existing policies.

AI Policy and Security Considerations

Quantify and Evaluate Your AI Implementation

GovTech Innovators

Define the Scope of AI Use

- Identify which processes will involve AI, the type of data AI systems will manage, and how these will impact decision-making processes.

Risk and Opportunity Assessment

- **Privacy Concerns:** Data usage and potential exposure.
- **Bias and Discrimination:** Risks related to biased AI outputs and ways to mitigate them.
- **Security Vulnerabilities:** Ensuring adequate protection for AI systems.
- **Efficiency Gains:** Areas where AI can enhance productivity or reduce manual work.
- **Note:** Consider department-specific factors and tailor the AI Use Policy based on department size, technical capabilities, data sensitivity, and available resources.

AI Policy and Security Considerations

Gap Analysis

What is a Gap Analysis?

- Identify, document and categorize all gaps between existing policies and the necessary policy components of AI Use.

Detailed Gap Analysis

- **Purpose and Scope:** Ensure existing policies clearly define the intent and scope of AI integration, specifying areas where AI will be applied.
- **Guiding Principles:** Align current ethical guidelines with AI use, emphasizing fairness, accountability, and transparency.
- **Data Governance:** Evaluate whether current data governance protocols address AI needs, including data storage, usage, and retention.
- **Permitted and Prohibited Uses:** Ensure acceptable use policies cover AI-specific applications and limitations.

AI Policy and Security Considerations

Gap Analysis - Continued

Detailed Gap Analysis

- **Transparency and Bias Mitigation:** Confirm if current policies ensure transparency in AI decision-making and prevent bias.
- **Security Protocols:** Verify if current IT security policies are sufficient for AI systems, including encryption, access control, and threat monitoring.
- **Human Oversight:** Determine if human oversight mechanisms are adequate for AI outputs, including regular reviews.
- **Incident Response:** Confirm if response plans cover AI-related incidents, such as data breaches or ethical violations.
- **Compliance and Legal Standards:** Ensure compliance policies meet regulatory standards, such as data privacy and ethical requirements.
- **Training and Awareness:** Verify if training programs address AI awareness, its benefits, and associated risks.

AI Policy and Security Considerations

AI Policy Approaches

Amend Existing Policies

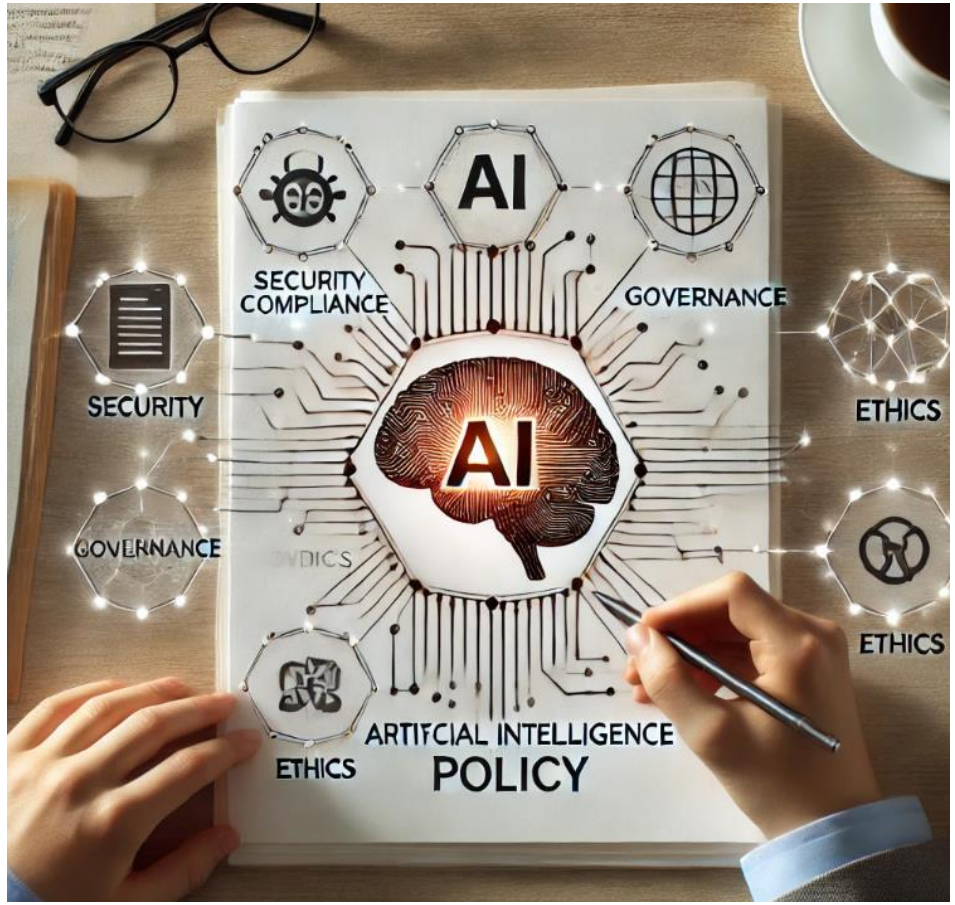
- **Suitable For:** Departments with comprehensive, up-to-date policies that can accommodate AI.
- **Alignment:** Where AI use aligns well with existing technology use policies.

Create New AI Use Policy

- **Suitable For:** Scenarios where the necessary policy component doesn't integrate well into existing policy.

Hybrid Approach

- **Suitable For:** Scenarios where some policy components can be incorporated into existing policies while others require the development of new AI-specific policies.



AI Policy and Security Considerations

Develop or Amend Policy

GovTech Innovators

Updating and/or Creating Policy

- **Update to Date Definitions:** Include AI-related terms to ensure consistency.
- **Extend Data Governance:** Incorporate requirements for handling data used or generated by AI.
- **Risk Mitigation Strategies:** Integrate specific risk management practices for AI.
- **Scope and Purpose:** Define AI use, specifying impacted processes and expected outcomes.
- **Guiding Principles:** Set ethical guidelines for AI use, focusing on fairness, accountability, transparency, and inclusiveness.
- **Data Governance:** Establish rules for data collection, storage, and processing for AI, including privacy protection for PII.
- **Permitted and Prohibited Uses:** Clearly define acceptable AI applications and areas requiring human oversight.

AI Policy and Security Considerations

Develop or Amend Policy - Continued

GovTech Innovators

Updating and/or Creating Policy

- **Transparency:** Make AI decisions transparent and provide guidelines for notifying stakeholders when AI is used.
- **Bias Mitigation:** Set protocols to prevent bias through diverse training data and regular audits.
- **Security:** Develop specific AI security measures, including encryption, access control, and threat monitoring.
- **Human Oversight:** Establish roles for staff in monitoring AI outputs, intervening as needed.
- **Incident Response:** Develop procedures for AI-related incidents, including reporting and remediation.
- **Compliance:** Align with relevant data protection and ethical standards, ensuring federal and state law compliance.
- **Training and Awareness:** Consider requiring training on the use of AI tools, covering capabilities, risks, and best practices.
- **Monitoring and Evaluation:** Set metrics to evaluate AI effectiveness, scheduling regular reviews for updates.

AI Policy and Security Considerations

AI Policy Considerations – Implement, Monitor and Iterate

GovTech Innovators

Develop and Roll Out Policy

- Train staff and implement the policy in phases, starting with low-risk areas.

Review Process

- Establish regular policy reviews and gather continuous feedback from staff and stakeholders.

Monitor and Iterate

- On an ongoing basis, monitor the performance of AI tools in your department, the effectiveness of your policy, revise and iterate to continuously improve

AI Policy and Security Considerations

Artificial Intelligence Roadmap

GovTech Innovators

What is the AI Roadmap?

- The AI Roadmap provides a strategic, step-by-step plan for incorporating Artificial Intelligence into Parks and Recreation departments.

Why is it so Important?

- **Structured Adoption:** The roadmap enables a structured and phased approach, minimizing disruptions and maximizing positive outcomes.
- **Risk Mitigation:** Identifies opportunities for improvement while proactively managing potential risks, such as data privacy and ethical concerns.
- **Alignment with Goals:** Helps ensure AI initiatives align with department objectives, leading to more effective and meaningful outcomes.
- **Resource Allocation:** A roadmap provides clarity on resource needs and helps departments allocate budgets efficiently for maximum impact.

AI Policy and Security Considerations

Artificial Intelligence Roadmap: Key Components

GovTech Innovators

Assessment and Planning

- Conduct an in-depth analysis of the department's existing technology, operations, and AI readiness.
- Define specific needs: streamlining processes, improving customer engagement, or both.

Organizational Alignment and Training

- **Staff Engagement**: Include staff from the outset to foster buy-in and reduce resistance.
- **Comprehensive AI Training:** Educate staff on how to use AI tools effectively, covering both capabilities and limitations. This includes understanding AI's benefits, how it fits into their daily work, and what kind of outputs they should expect.
- **Using AI to Troubleshoot AI:** Provide guidance on leveraging AI tools to identify and troubleshoot problems with AI-generated outputs. Staff should understand how to use iterative prompts to refine AI results and address inaccuracies.

AI Policy and Security Considerations

AI Roadmap: Key Components Continued

Implementation

- Start with low hanging fruit, such as AI-assisted marketing or program planning automation.
- Gradually scale up to incorporate AI across more complex operations, like resource allocation and financial management.

Risk Management

- Identify potential risks such as those noted earlier in this presentation, (data privacy issues, bias, operational disruption, etc.)
- Implement mitigation strategies as described earlier (transparent decision-making processes, manual oversight, and setting ethical use guidelines.)

Evaluation and Continuous Improvement

- Establish metrics for success, such as cost savings, improved service delivery, and time saved.
- Regularly collect feedback and use it for iterative improvements to maximize the roadmap's effectiveness.

AI Policy and Security Considerations

AI Roadmap: In Closing

Purpose

- Ensures a structured and methodical approach to implementing Artificial Intelligence in your department, assessing all risks and opportunities and selecting the optimal approach for your department

Supplements AI Use Policy

- Works best in tandem with an AI Use Policy.
- Should be developed in parallel with your AI Use Policy as a complimentary document.

Helps with Organizational Alignment

- Provides one central document for leadership and staff to reference for use of AI in your organization
- Focuses on how AI is to be used in your department, what tools to use, when to use them, training required before use of AI tools, risks and mitigation and continuous improvement

Your AI Journey

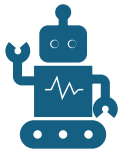
GovTech Innovators

Policy Development

Craft comprehensive policies to ensure ethical and effective use of AI.

AI Roadmap

Develop tailored roadmaps for integration of AI into your department's operations



AI System Engineering

AI System Design, Engineering and Support: Design, implement and support AI systems that deliver on your priorities

- Analyze current state and recommend AI solutions
- Automate and optimize by connecting disparate systems with AI

Training and Coaching

AI Training and Coaching: Provide training and ongoing support to ensure your team is well-equipped to leverage AI technologies

Questions?

Contact Us Today to Get Started!

www.govtechinnovators.com

jpeters@govtechinnovators.com

Phone: 517.862.4397