Cybersecurity and Artificial Intelligence Policy

Summary Policy Statement

The Orange County Sanitation District (OC San) is committed to building and maintaining resilient, secure, and ethically governed technology systems. This includes a robust cybersecurity posture and the responsible adoption of Artificial Intelligence (AI), including both generative AI and advanced operational AI. As OC San advances its digital transformation, the agency must ensure that its technology practices safeguard data, systems, and operations, while also leveraging innovation to improve service delivery, operational efficiency, and decision-making. This policy outlines OC San's dual approach: securing our digital assets from evolving threats and strategically implementing AI in a phased, ethical, and transparent manner aligned with organizational goals.

Background

Cybersecurity has become an increasingly complex challenge for all public agencies. Threats from nation-states, cybercriminals, and insider risks continue to grow in scale and sophistication. At the same time, the rapid rise of artificial intelligence — particularly generative AI like ChatGPT and Microsoft Copilot — presents both powerful tools for operational efficiency and significant ethical, legal, and cybersecurity risks.

OC San recognizes the need for continuous improvement in both cybersecurity readiness and AI maturity. Cybersecurity must be embedded across all technology layers, and AI must be introduced through a structured governance framework that supports safe and equitable innovation.

Current Situation

Cybersecurity

OC San has significantly expanded its cybersecurity capabilities over the past several years. OC San now maintains a 24/7 Security Operations Center (SOC)-as-a-Service, staffed security roles, and a comprehensive portfolio of protection measures, including:

- Security Awareness & Training: Quarterly training, phishing simulations, and targeted sessions for IT and engineering teams.
- Vulnerability Management: Continuous scanning and patching supported by threat intelligence from US-CERT, ICS-CERT, and others.
- Intrusion Detection & Response: Tools include firewalls, behavior analytics, web gateways, and next-gen anti-malware.

- SOC Monitoring: Around-the-clock threat monitoring for network reliability and integrity.
- Privileged Access Management: Tools to control and audit administrative access.
- Data Backup & Disaster Recovery: A 3-2-1-1-0 strategy with monthly restore testing.
- Security Incident Response: Playbooks and partnerships with DHS, FBI, and private incident response firms.
- Security Assessments: Regular third-party security reviews and red team exercises.

Artificial Intelligence

OC San is in the early stages of AI implementation, following a "crawl-walk-run" maturity model to ensure thoughtful and responsible adoption. Current activities include:

- AI Use Guidelines: Initial generative AI use policy established and aligned with HR Policies and Procedures.
- AI & Data Analytics User Group: A cross-functional team exploring and piloting use cases.
- Pilot Programs: Microsoft Copilot and ChatGPT pilots underway to improve office productivity.
- Trends & Education: Ongoing training based on insights from Microsoft, Gartner, and industry groups.

AI is being approached in two distinct categories:

- Generative AI — Focused on content creation (e.g., text, code) to support administrative and communication functions.
- Operational AI — Used for predictive analytics, SCADA optimization, video input, and equipment monitoring.

Future Policy Direction

Looking ahead, OC San will continue to strengthen and evolve its cybersecurity and artificial intelligence capabilities to meet the demands of a rapidly changing technological landscape. Cybersecurity incidents are no longer a question of "if" but "when," and OC San is committed to building a resilient security program that anticipates threats and responds effectively. This includes continuous refinement of its threat detection, incident response, and recovery protocols. At the same time, the agency will expand its AI capabilities beyond pilot programs, with a focus on operational

applications such as predictive maintenance, real-time process optimization, and intelligent video surveillance. A phased AI maturity model—moving from foundational awareness to full-scale implementation—will guide this progression, ensuring that each stage builds the necessary governance, technical expertise, and ethical safeguards.

As both cybersecurity and AI continue to evolve, OC San will align its strategies with emerging best practices and maintain governance frameworks that address key risks such as data privacy, misinformation, algorithmic bias, and system integrity. By integrating security and innovation, OC San aims to responsibly adopt new technologies that enhance service delivery and protect public trust.

Initiatives to Support Progress Toward the Policy Goal

To support the continued advancement of both cybersecurity and AI, OC San will pursue the following initiatives:

Cybersecurity Initiatives

- Conduct tabletop exercises to test and improve incident response readiness.
- Expand SOC capabilities and automation to support real-time threat protection.
- Perform ransomware readiness and third-party red team assessments.

AI Initiatives

- Implement a phased AI resourcing plan leveraging support from Microsoft and Gartner.
- Launch awareness campaigns and targeted training for Microsoft Copilot and other AI tools.
- Evaluate AI infrastructure options (e.g., hosted vs. on-premises).
- Expand operational AI use in areas such as SCADA, asset health monitoring, and CCTV analytics.
- Continuously update generative AI policy to reflect advancements and align with OC San values.