Date Filed: October 22, 2026

Witness: Christopher Leigh and Sean P. Noonan
Request from: ALLCO

Question:

(Policies governing employees and executives.) Produce each policy, standard, guideline, directive, or training material in force at any time since January 1, 2024 that governs the use of AI Tools by Company or ESC employees, officers, or executives, with its effective date and the person by title who approved it, and state: (a) whether employees, officers, or executives who have access to confidential information, customer information, or CEII are prohibited from using any AI Tool; (b) if they are not prohibited, what categories of information may and may not be entered into which AI Tools, and the safeguards (enterprise tenancy, no-retention and no-training terms, data-loss-prevention controls, access logging, or otherwise) the Company relies upon; (c) whether any officer or executive of the Company or of Eversource Energy — including the Chief Executive Officer, the Chief Financial Officer, the General Counsel, and the witnesses sponsoring testimony in this docket — uses any AI Tool in the course of his or her duties, and which; (d) whether the Company has ever determined that an employee, officer, or executive entered confidential information, customer information, or CEII into an AI Tool, and what action was taken; and (e) whether the Company contends that State of Connecticut Policy AI-01 (AI Responsible Use Framework, Feb. 1, 2024) applies to the Company, its employees, or its Contractors, and the basis for that contention.

Response:

Eversource's requirements for the use of artificial intelligence are part of the Company's broader information security and risk-management framework. These requirements apply to Company personnel generally, including employees, officers, and executives. Officers and executives are subject to the same restrictions as other personnel regarding approved AI tools, appropriate data handling, protection of confidential and regulated information, and validation of AI-generated output. The principal governing document is the IT Risk Management Policy, Section 02.7, Artificial Intelligence Security. The Vice President and Chief Information Security Officer sanctions all IT Policy revisions.

Eversource supplements these policies with training and awareness materials. These include AI at Eversource. Training covers approved AI tools, AI risks, employee responsibilities, human accountability, and safe submission of AI ideas. Training is supplemented via Microsoft Learn, an asynchronous learning platform, as well as tool specific training such at Copilot Chat 101.

(a) Access to confidential information, customer information, or CEII

Employees, officers, and executives may use AI capabilities that Eversource has reviewed, approved, licensed, and provisioned for their work, subject to Company security and information-handling requirements.

Company data may only be entered into approved AI tools in accordance with Eversource's data-classification and security requirements. Highly Restricted information and other prohibited data, including CIP, CEII, protected or confidential personal information, security credentials, and attorney-client privileged information, may not be entered into AI tools such as Copilot Chat.

(b) Permitted information, prohibited information, and safeguards

Under the current policy, approved enterprise AI tools may be used for appropriate business-productivity activities, including drafting, summarizing, brainstorming, and analysis, provided that the information is appropriate for the tool and permitted under Eversource data-classification requirements. AI-generated work must be reviewed by a qualified person for accuracy, completeness, and appropriateness before it is relied upon or distributed.

Absent explicit approval from the Enterprise AI Team, personnel may not enter, upload, or process in an AI system:

- Highly Restricted information;
- Confidential Business Information;
- Protected or Confidential Personal Information;
- Critical Infrastructure Protection information;
- Critical Energy Infrastructure Information;
- Security credentials, keys, or authentication data; or
- Attorney-client privileged information.

The approved enterprise AI tools include Microsoft 365 Copilot, Microsoft 365 Copilot Chat, and approved Microsoft Foundry models. Public or third-party AI tools that lack an enterprise agreement and a unique Eversource tenant are treated as public AI systems and are prohibited for Company work or Company data unless expressly approved through Eversource's security and AI governance processes.

Depending on the applicable platform and use case, Eversource's safeguards include enterprise-controlled environments; data-classification and sensitivity-label controls; data-loss-prevention protections for prompts and uploaded content; least-privilege and role-based access; encryption; audit logging; monitoring and alerting; security testing; human validation; and formal review of third-party tools, connectors, plug-ins, APIs, and integrations.

(c) Use by officers and executives

Eversource does not establish a different AI-use standard for officers or executives. Any officer or executive using an AI tool for Company work is subject to the same approved-tool, information-classification, security, human-review, and validation requirements as other Company personnel.

(d) Determinations involving impermissible information

Eversource's policies provide for auditing, monitoring, and enforcement. Depending on the circumstances, policy noncompliance may result in blocked activity, revocation of AI access, remediation requirements, investigation, or disciplinary action under applicable Information Security and Human Resources processes.

(e) Connecticut Policy AI-01

Eversource governs its use of AI through its own information security, risk-management, data-classification, vendor-risk, and AI governance requirements, together with applicable laws, regulations, and contractual obligations.