conEdison
a conEdison, inc. company

Mary Krayeske
Assistant General Counsel
Law Department

November 16, 2026

VIA ELECTRONIC FILING

Honorable Michelle L. Phillips
Secretary
New York State Public Service Commission
Three Empire State Plaza
Albany, NY 12223-1350

Re: CASE 26-M-0552 - Artificial Intelligence Utilization in the Operations of Public Utilities and Other Regulated Entities.

Dear Secretary Phillips,

Artificial Intelligence (AI) is transforming the technology landscape, with AI capabilities becoming embedded across the tools, platforms, and services that support the utility industry. At the same time, frontier AI models are rapidly advancing, making smarter and faster tools available. As these capabilities develop, Consolidated Edison Company of New York, Inc. (Con Edison) and Orange and Rockland Utilities, Inc. (O&R, together, the Company) recognize that AI offers meaningful benefits when appropriately applied to business needs. The Company understands that AI use and its associated risks must be properly governed as AI becomes an integral part of the Company's technology landscape. The Company looks to use AI where it improves efficiency, speeds development and makes sense. The Company is developing governance and other processes to assist with AI deployment and evaluating where and how it can provide meaningful benefits.

In 2023, the Company realized AI's potential and issued AI Guidelines that established expectations for responsible AI use. As AI developed and matured, and the Company's AI use expanded, the Guidelines were formalized into Corporate Policy CEI-311, *Artificial Intelligence Policy* (*AI Policy*). The Company continues to build on this foundation through governance processes designed to support the responsible use of AI as its capabilities and applications evolve.

As technology evolves, the Company expects that its use of AI and the governance around it will also evolve. The Company welcomes the opportunity to work with DPS Staff and the Commission on this emerging technology.

Current AI Use Cases

Between Con Edison and O&R, the Company currently has 25 AI use cases in operation. They generally support two areas: business operations, where AI supports specific business processes, such as enabling Customer Service Representatives to quickly find and understand relevant guidance during customer interactions, and operational enablement, where AI strengthens the technology, data, and enterprise capabilities that support how work is performed across the organization. The Company has several use cases in development and expects that in the near future, the number of use cases that assist employees in providing better service to customers will increase. *Attachment 1* provides the Company's current inventory of operational AI use cases, including the AI system on which each use case is built, its functional objective, and the level of human oversight.[1]

Existing Technology Review Processes

The Company has a process for evaluating AI use cases and platforms. *Attachment 2* provides the Company's process for technology review, development, testing, approval, and deployment. Corporate Policy CEI-215, *Acquisition, Deployment and Support of Information Technology*, establishes requirements governing technology implementations, including the software development lifecycle and registration of technology-related projects with the Company's Enterprise Technology and Security group. Additionally, the Company's *Corporate Request for Evaluation & Approval of Technology (CREATe)* process manages the technical review for new technology or a change in existing design architecture. These processes provide a structured mechanism for identifying relevant technology, security, data, privacy, and other considerations throughout the software development lifecycle.

AI Governance Framework

The Company is incorporating an Artificial Intelligence Development Lifecycle component, including AI governance and risk tiering, into CEI 215, the software development lifecycle, and CREATe. This integration is intended to help identify AI-enabled

[1] Two of the use cases are considered confidential and an unredacted version of this filing has been provided to the Records Access Officer.

solutions within the existing technology lifecycle and apply governance considerations based on the nature and risk of the AI use.

Attachment 3 provides the Company's framework for the responsible development and ethical use of AI.[2] The AI Policy establishes the enterprise governance framework, supported by guidance, technology requirements, and risk-based governance controls addressing human oversight and override, testing and validation, monitoring, and AI lifecycle governance. It defines the expectations that guide responsible behavior and decision-making when designing, using, and relying on AI across the Company and promotes human accountability, risk awareness, and use aligned with Company values.

The Company's AI governance structure provides oversight, strategic guidance and operational support to the Company's AI projects. Building on the AI Guidelines, in 2026, the Company established a formal three-level AI governance structure designed to provide operational, management, and executive oversight of AI. The governance structure consists of:

- **AI Governance Working Group**, which, through ongoing meetings, supports the day-to-day operation of the AI governance program, including visibility into the AI portfolio, governance tiering, standards, controls, and lifecycle checkpoints;
- **AI Operating Group**, a Vice President-level body that meets monthly and provides management oversight, promotes consistent application of AI governance across functions, and reviews and escalates significant risks and exceptions; and
- **AI Executive Oversight Committee**, a Senior Vice President-level body that meets every other month and provides enterprise-level direction and oversight, reviews AI governance reporting, and addresses escalated matters and policy exceptions.

Additionally, as noted in the AI Policy, the Company is implementing a risk-based process for evaluating AI use cases and assigning an AI Governance Tier based on the intent, purpose, and potential impact of the use case. The assigned tier is intended to inform the level of governance oversight and applicable controls. The risk tiers and oversight models include:

[2] Also included in the document are the Company's original and updated AI Guidelines.

AI Governance Tiers and Oversight

Tier	Tier Description	Oversight Model	Examples
Tier 1 – Standard Approval	AI systems with limited operational impact that support internal productivity and do not influence consequential business, customer, safety, or regulatory decisions.	Periodic / Ad Hoc Human Oversight: Humans remain responsible for final use of AI outputs. No autonomous operational actions.	Drafts internal content for employee review using an approved enterprise tool.
Tier 2 – Approval with Conditions	AI systems that support business processes, customer interactions, or operational decision-making and require enhanced governance oversight.	Human-on-the-Loop: Active monitoring is required, with authorized personnel able to intervene, override, or suspend activity before consequential actions.	Analyzes operational data and recommends actions requiring human validation.
Tier 3 – Active Oversight	AI systems that impact customers, employees, reliability, safety, regulated activities, or other business-critical functions and require formal governance review and ongoing oversight.	Human-in-the-Loop: Human review and approval are required before consequential outputs or actions take effect, with formal escalation, monitoring, override, and accountability controls.	Supports customer, reliability, safety, or regulatory decisions under active oversight.
Tier 4 – Executive Determination	AI systems presenting significant enterprise, legal, regulatory, ethical, reputational, or control considerations that require senior executive review and determination prior to implementation.	Executive Determination: Senior executive review is required before implementation. If approved, oversight and controls are established based on the use case and associated risks.	Initiates or materially influences decisions with significant enterprise implications.

AI and the Company's Data Privacy Program

The Company is building on its existing privacy and data protection requirements as a foundation for addressing privacy considerations associated with AI. As AI use cases are

evaluated, the Company leverages existing privacy review and assessment processes to help identify relevant considerations and appropriate safeguards. This approach provides a starting point for identifying and addressing privacy risks as the Company's use of AI continues to evolve. *Attachment 4* includes the Company's policy on the definition and handling of Personally Identifiable Information, and other policies defining the Company's framework for data classification, protection, and information management.

Conclusion

The Company is committed to the responsible and transparent use of AI, with governance, controls, and human accountability appropriate for the use case's purpose, potential impact, and risk. The Company's approach builds on established technology review, cybersecurity, privacy, and data governance processes and adds AI-specific policies, risk-based governance, and defined operational, management, and executive oversight. As AI technologies and their potential utility applications continue to evolve, the Company expects to continue refining its governance framework and controls based on experience, evolving risks, industry practices, and applicable regulatory requirements.

Respectfully submitted,

Attachment 1
REDACTED

AI use-case inventory (25)

Use Case Name	System	Use Case Description	Functional Objective	Level of Human Oversight	Business Operations or Operational Enablement
Knowledge Advanced AI	Oracle Knowledge Advanced	Customer Operations uses Customer Care and Billing (CC&B), an Oracle customer information system, to handle the Company's meter-to-cash process, including allowing Customer Service Representatives and other employees to access customer account information. Oracle Knowledge Advanced is an Oracle product that provides Customer Service Repreentatives and other employees with information about the customer service process. This includes access to support articles and guidance. From Oracle Knowledge Advanced, the Company built a generative-AI natural-language search and summarization tool, allowing Oracle CC&B users to ask questions in everyday language, retrieve relevant information, and receive concise summaries for use during customer interactions. This capability improves the quality of the customer service interaction. This project is included in the Company's Back Office Automation report.	Enable employees using CC&B to find and understand relevant support guidance more quickly during customer interactions, and improving the consistency and quality of the customer service interaction.	Level 1 - User Validation	Business Operations
eGIS AI Search	Azure OpenAI	The Enterprise Geographic Information System (eGIS) is a mapping and visualization platform used to locate and manage information about Company assets and support system operations. The eGIS Knowledge Hub contains guidance and knowledge articles used by employees who work with eGIS. The eGIS AI Search capability was built and implemented using Azure OpenAI to allow users to search the full content of Knowledge Hub articles, ask questions in everyday language, and receive summaries based on the inquiry. The solution also includes the cloud infrastructure, website interface, data connections, chat capability, testing, production launch, and ongoing support needed to operate the solution. The project's capability has been expanded to use Azure OpenAI and Azure AI Search to let users search the full content of the articles, ask questions in a chat interface, receive answers grounded in the Knowledge Hub, and return to prior conversations. The platform is also designed to support connections to additional eGIS and enterprise information sources.	Make eGIS information easier to find and understand by allowing users to search article content and receive concise, source-based summaries as well as increase performance and allow users to see search history.	Level 1 - User Validation	Business Operations
Oracle AI Generative Capability through Upgrade	Oracle HCM	Human Resources uses Oracle Human Capital Management (HCM) products to support employee administration, such as time, payroll, training, compensation, and career development. Oracle provides various generative-AI and agent-assistance features to assist in these process. These features can answer employee questions, especially through the self-service features, route cases, assist HR representatives, and draft knowledge articles. The capability is intended to reduce manual work, improve knowledge reuse, and help resolve employee questions.	Reduce Human Resources resolution time by expanding employee self-service and assisting Human Resources staff throughout the case-management process.	Level 1 - User Validation	Business Operations
PERSUIT AI Features	PERSUIT	The Law Department purchased PERSUIT to create and manage requests for proposals from outside law firms and to compare the responses received. PERSUIT also provides an AI features that can automate parts of the proposal workflow, compare proposed pricing with benchmarks, and recommend law firms. These capabilities are intended to make the sourcing process more consistent as well as quicker, improve the user experience, and support management of outside legal costs.	Improve the speed, consistency, and cost effectiveness associated with selecting and managing outside legal services.	Level 1 - User Validation	Business Operations

Use Case Name	System	Use Case Description	Functional Objective	Level of Human Oversight	Business Operations or Operational Enablement
General Litigation Research Agent	Microsoft CoPilot	General Litigation attorneys review previously filed motions, court orders, and case briefs manually when researching legal issues or drafting new motions. An internally-developed Copilot research assistant searches these materials based on an attorney's description of the issue and returns relevant examples, arguments, and concise summaries. For example, an attorney preparing a summary-judgment motion can use the assistant to identify earlier motions and orders involving similar facts. The capability reduce document-by-document research time while giving attorneys faster access to potentially useful prior work.	Assist General Litigation attorneys to locate relevant prior motions, orders, arguments, and case materials for research or drafting documents.	Level 1 - User Validation	Business Operations
Orange and Rockland Good Catch/Close Call	Azure Open AI	Orange and Rockland receives reports of near misses for safety that must be revwied and categorized as either a good catch, a close call, or not eligible under the applicable criteria. The implemented Azure OpenAI solution reviews each submission, applies defined logic and AI-based analysis, assigns a category, and supports tracking and reporting. The capability is intended to reduce manual sorting and improve consistency in how safety submissions are classified.	Classify and track near miss safety reports more efficiently and consistently for Good Catch and Close Call reporting.	Level 1 - User Validation	Business Operations
Vehicle Idling Data Science Solution	Google Cloud Platform and Google Gemini	The Company receives vehicle-idling penalties based on citizen-submitted video evidence. Company personnel must determine whether each video includes required information, such as a visible date and time, the vehicle's license plate, and evidence that the engine was running. A solution using Google Cloud Platform and Google Gemini assists with reviewing the videos and organizing the results for an dispute workflow. The capability reduces manual review time and identifies penalties that may have grounds for dispute.	Review vehicle-idling evidence more efficiently and identify cases that may qualify for dispute, with the goal of reducing avoidable penalty costs.	Level 3 - Embedded Review	Business Operations
Meter-To-Transformer Mapping	C3 AI Generative AI (agentic platform)	Company records identify approximately 70,000 to 76,000 meters with potential meter-to-transformer mapping inaccuracies, with about 120,000 additional meters having uncertain mappings. The implemented C3 AI solution analyzes smart-meter voltage patterns, outage signals, and GIS network information to identify possible mismatches without waiting for an outage. It recommends the most likely transformer, assigns a high, medium, or low confidence rating, and provides supporting evidence for engineering review. More accurate mappings are intended	Identify and addess meter mapping inaccuracies	Level 3 - Embedded Review	Business Operations
Discovered Meter Image Scanning	Azure Open AI	This AI project performs two functions: (1) it digitizes all existing manual meter records, and (2) reviews and analyzes photographs of utility meters to assist employees in identifiying meters, by extracting relevant meter details. The project provides a meter record database as well as reduce manual image review and make usable meter information available more quickly.	Implement a meter database and extract relevant information from meter photographs.	Level 1 - User Validation	Business Operations

Use Case Name	System	Use Case Description	Functional Objective	Level of Human Oversight	Business Operations or Operational Enablement
COInsight - Procurement	Azure Open AI	COInsight is a agent that helps Supply Chain manage Certificates of Insurance (COI). The tool determines if a vendor's COI meets Company coverage requirements and risk classifications by scanning each certificate, ereviewing policy and coverage information, and comparing the results with internal requirements. The capability is intended to reduce manual document review and data-entry errors and help Supply Chain identify missing or noncompliant insurance information.	Automate the extraction and review of Certificate of Insurance information so Procurement can identify compliance issues.	Level 1 - User Validation	Business Operations
SCOP Guide	Azure Open AI	Supply Chain employees rely on operating procedures and Corporate Instructions covering procurement, risk assessment, inventory management, ethical sourcing, supplier diversity, approval authority, and compliance. The Supply Chain Operations (SCOP) Guide searches these approved documents and provide summaries or answers to employee questions. The capability helps employees find and apply the correct procedures without manually reviewing lengthy documents.	Help Supply Chain employees quickly locate, understand, and apply the correct operating procedure or Corporate Instruction.	Level 1 - User Validation	Business Operations
Policy Document Process - AI Builder Flow	Microsoft Power Platform	Compliance specialists currently review policy, procedure, and regulatory documents manually or use predefined keyword searches to identify controls, obligations, and requirements. This enhancement extends the existing Compliance Policy Parser with Microsoft AI Builder document processing. The solution reads uploaded documents, extracts relevant compliance text, and presents the results in a structured format for specialist review and downstream use. The capability is intended reduce review effort and improve consistency.	Assist Compliance specialists with identifying and organizing control activities, obligations, and requirements in policy and regulatory documents.	Level 3 - Embedded Review	Business Operations
Trimble Connect Desktop Application	Azure Open AI	Research and Development worked with a vendor, using NYSERDA funding, to develop a digital replica 4 Irving Place, including the building and its HVAC system. The tool recommends operational changes, e.g., close valves, change zone temperatures, to reduce energy usage in real time as well as maximize waste heat recovery. Additionally, the tool will assist with strategic decisions related the Company's compliance plan for New York City Local Law 97.	Support building-energy analysis, emissions-reduction planning, and development of a Company compliance plan for New York City Local Law 97.	Level 1 - User Validation	Business Operations
AI Vehicle Idling	Microsoft Power Automate	Orange and Rockland Operations collects vehicle-idling information from Company yards and reviews monthly trends to identify possible concerns. The implemented solution uses AI to analyze changes over time and highlight locations and times of day with recurring or increasing idling. Power Automate places the findings into a draft email for human review before it is sent to supervisors. The capability is intended to reduce analysis and reporting effort while supporting targeted follow-up.	Help supervisors identify recurring vehicle-idling concerns by automating monthly trend analysis and preparation of reviewable communications.	Level 1 - User Validation	Business Operations
Personal Stakeholder Agent Indentifier	Microsoft Copilot Studio	ETS - Shared Services serves at least 20 Company organizations at CECONY and O&R. They maintain a list of clients (greater than 100 people) that must be updated when employee roles change. A Copilot Studio assistant compares the list with authorized Microsoft 365 or Teams profile information, including current job titles, and identifies records that may no longer reflect the appropriate stakeholders. The capability helps reduce the time required to review the list and help keep stakeholder information current.	Reduce manual review of the stakeholder list by identifying records that may need to be updated based on current employee information.	Level 1 - User Validation	Business Operations
Engineering Automation	Microsoft Copilot Studio	Using CoPilot Studio, Central Engineering has automated reminder emails for certain tasks, e.g., timesheets. The capability helps reduce repetitive preparation work.	Automate recurring weekly emails.	Level 1 - User Validation	Business Operations

Use Case Name	System	Use Case Description	Functional Objective	Level of Human Oversight	Business Operations or Operational Enablement
Strategic Planning EA Agent	Microsoft Copilot Studio	The Strategic Planning Executive Assistant coordinates changing tasks, meetings, agendas, speakers, and follow-ups across senior leadership. A Copilot Studio assistant connected to Microsoft 365 helps update Excel trackers, organize calendars, monitor meeting details, send reminders, and identify coordination issues as schedules change. The capability is intended to reduce manual administrative work and improve the accuracy and timeliness of leadership coordination.	Support the executive assistant by automating and organizing Strategic Planning meeting, task, schedule, and follow-up coordination.	Level 1 - User Validation	Business Operations
Gas Leak Call Analytics	C3 AI and Microsoft Power Business Intelligence (BI)	The Gas Emergency Response Center (GERC) plans field resources for gas-leak emergencies using historical call activity, current operating conditions, weather, planned work, and supervisory judgment. Gas Leak Call Analytics uses C3 AI to forecast expected call volumes by work shift and geographic area and display historical and forecast information through Gas Central Reporting. The forecasts provide an additional planning input for crew positioning and readiness, while operational decisions remain with GERC supervision and management.	Improve emergency-response planning by forecasting gas-leak call volumes to support crew positioning and resource readiness.	Level 1 - User Validation	Business Operations
Data Activation (Maximo)	Oracle	Oracle products contain a Data Distribution Hub (DDH), which connects systems that produce data with systems that consume the data. The DDH moves data into one location for future use, such as reporting and analysis. The initiative supports the build of a construction data lake that will include construction work from Maximo as well as finanical data. Once the data lake is vetted for quality, Construction will be able to perform analytics on the data, including work-order review and possible construction-fraud detection.	Make approved data available for analytics, including work-order reporting and fraud-detection use cases.	Level 1 - User Validation	Enterprise Enablement
Solution NameAsset Inventory Assistant	Microsoft Copilot Studio	Security personnel previously manually searched Excel files to identify IT and OT assets, confirm the organization the assets were assigned to, and/or update the actual location of the equipment. A Copilot Studio assistant in Microsoft Teams lets a technician attach a photograph of an asset's serial-number label. The assistant reads the label and through Excel, provides the needed information, including the asset owner and location.	Give technicians a faster, mobile-friendly way to identify assets, confirm assignments and locations, and record location changes.	Level 1 - User Validation	Operational Enablement
Tableau to Power BI GenAI Conversion Tool	Google Cloud Platform	The Company is retiring Tableau and moving thousands of dashboards across multiple business units to Microsoft Power BI. An internal generative-AI tool allows a user to upload a Tableau workbook and receive a detailed migration guide. The tool generates a converted Power BI project file and provides chat-based assistance during conversion. The capability is intended to reduce the time, effort, and cost required for the enterprise dashboard migration.	Accelerate and standardize the conversion of Tableau dashboards to Power BI while reducing migration effort and cost.	Level 1 - User Validation	Operational Enablement
Gemini Enterprise + Microsoft O365 Integration	Google Gemini	Employees store and work with Company information in Microsoft 365 applications. This project connects authorized Microsoft 365 data to Gemini Enterprise, allowing users to use Gemini capabilities with information they are permitted to access. Depending on the configured functions, users can search, summarize, and work with Microsoft 365 content through Gemini while retaining existing access controls.	Allow authorized employees to use Gemini Enterprise with Microsoft 365 information they already have permission to access.	Level 1 - User Validation	Operational Enablement
AI Tool for Research Center Anthology	Azure Open AI	The Research Center, which is available to all employees, maintains research materials that employees may need to locate, review, and understand. This AI solution collects research content, organizes it by topic, and prepares concise summaries in a centralized anthology. The capability intends to improve access to prior research, speed knowledge discovery, and make the documentation of research insights more consistent.	Create a centralized, organized, and summarized collection of Research Center materials so employees can find and understand prior research more quickly.	Level 1 - User Validation	Operational Enablement

Attachment 2

CEI-215 Acquisition Deployment & Support of Information Technology –

Software Development Life Cycle Guide

Technical Review Procedure (CREATe)

conEdison, inc.

Corporate Instruction

SUBJECT

CEI-215 CI Acquisition Deployment and Support of Information Technology

1.0 PURPOSE -- This Instruction establishes Corporate standards for the acquisition, deployment, and support of information technology. Adherence to this Instruction is required to address the increasing reliance on information technology, growing interdependencies of applications and data, and cybersecurity threats.

2.0 APPLICATION --

2.1 This Corporate Instruction applies to the following Consolidated Edison, Inc. (CEI) subsidiaries and all organizations of Consolidated Edison Company of New York, Inc. (CECONY); Orange and Rockland Utilities, Inc. (O&R); and Con Edison Transmission, Inc. (CET). The terms Corporate or Company when used in this Instruction refer to CECONY, O&R, and CET unless otherwise stated.

2.2 This Corporate Instruction is applicable to IT projects. All organizations are subject to compliance with this Instruction regardless of whether the Information Technology (IT) organization actively performs the project management role for a given project and/or is responsible for the acquisition, or the organization performs that role itself or IT and the business are following a shared ownership application model.

3.0 DEFINITIONS --

3.1 Business – Organizations other than IT. They can be the sponsoring organization.

3.2 Business Lead – A person representing the business who bears responsibility for the successful delivery of project objectives.

3.3 Business Relationship Manager – An IT Manager who is responsible for developing and maintaining effective relationships between IT and the business units, and advocates for business needs within IT.

3.4 Client IT – People or groups in the business (not the IT organization) that manage applications or provide IT support without a designated IT employee assigned as an owner. Client IT are subject to IT's Corporate Instructions, policies and procedures, and they need to maintain accurate information in ServiceNow (SNOW) the IT work management system and asset repository for all company applications and technology infrastructure.

3.5 Enterprise Architect - Enterprise Architects provide standards, guidance, and governance for analyzing, designing, planning, and implementing required business & technical capabilities to successfully execute on business strategies.

3.6 **Information Technology** - Information and communication systems, applications, databases, platforms, and infrastructure, including cloud technologies and Operational Technology (OT) systems and devices.

3.7 **IT Lead** - A person representing the IT organization who bears responsibility for the successful delivery of project objectives. This person is also specifically responsible for adherence to IT procedures and processes relevant to the project. This could be a Systems Manager, Business Relationship Manager, Enterprise Architect, or other IT employee.

3.8 **Project** - A time limited endeavor to produce a unique service, asset, or result. A project can be a standalone initiative or part of a program. IT Projects are initiatives that involve the development, acquisition, and deployment of information technology. This could include new technology, upgrades/enhancements of existing technology, subscriptions/licenses, and an ongoing support model. IT capital projects must include, at a minimum, documentation of planning, design, development, testing, implementation, delivery, and maintenance & support.

3.9 **Project Manager** – Individual leading project management activities on behalf of the project; this could be the IT Lead or the Business Lead or a shared ownership model.

3.10 **Project Sponsor** – The person who sponsors the project on behalf of their organization. The sponsor establishes the vision and scope of the project and supports overall project objectives. They also ensure budget and resource availability.

3.11 **SDLC –** Software Development Lifecycle. This is a framework that defines the steps involved in the development of a technology solution, with detailed activities and ownership of each.

3.12 **Systems Manager** – An IT manager who advises on and/or oversees aspects of system design, development, implementation, and post-implementation support.

4.0 PROCEDURES --

4.1 **Funding Approvals –** Increases in capital project authorizations, new project authorizations, or increases in the total capital budget will be approved in accordance with the following procedures. (Reference CEI Corporate Instruction CEI CI-101, “Budgeting and Financial Forecasting.”)

a. CECONY. As specified in CECONY Corporate Policy Statement 000-1, “Delegation of Authorities,” and CECONY Corporate Instruction CI-610-1, “Capital Budget Process.”

b. O&R. Capital project authorizations and appropriations will follow the procedures described in O&R Policy 1.12, “Delegation of Authorities,” and CB-1, “Capital Authorization, Appropriation, and Funding Procedure.”

c. CET. Requests for increases in CET's capital project authorizations, new project authorizations, or increases in the total capital budget that require CEI Board approval will be sent to Financial Forecasting, Business Finance (CECONY), for review. Any increases will be approved in accordance with the CEI and CET Delegation of Authorities.

4.2 Project Registration --

a. CECONY and O&R. Each project must be registered with IT by the Project Manager to support strategic alignment and transparency. The registration will allow IT to review the project from different perspectives, including but not limited to design, solution architecture, and cyber security. Following successful review, submitters will receive approval of the proposed project so it may proceed to the next stage in the process. Steps to register projects are detailed in the IT Project Registration Procedure.

b. CET. Projects for CET, including its subsidiaries and investment companies, must register with IT by the Project Manager to support strategic alignment and transparency if deemed required by the Chief Information Security Officer, VP IT Engineering and Operations, or delegate, after a risk and materiality assessment is performed.

4.3 Project Management -- All IT capital projects must follow the IT Capital Project Management Procedure for the execution of IT capital projects. Furthermore, a formally accepted project management methodology (e.g. Waterfall, Agile), as well as a software development methodology, when applicable (SDLC), must be used to manage information technology projects.

4.4 Development of Support Model – As part of project planning, a support model must be furnished. This model should include estimating Capital/O&M budgets for maintaining the Information Technology, and planning for ongoing support contracts, license/subscription models, monitoring, and production support labor and/or other maintenance agreements.

4.5 Retention of Project Records - Project information must be kept for each project and retained in the project records and be readily available for review. Project records retention must comply with the requirements established under CECONY Corporate Instruction CI-870-1, "Records Management" or O&R Policy 5.14, "Records Management and Retention."

4.6 Policy Compliance - All IT projects covered by this Instruction must comply with the policies established under CECONY Corporate Policy Statement 310-2, "Computer Data Security"; CEI Corporate Instruction CEI CI-210, "Compliance with Section 404 of the Sarbanes-Oxley Act of 2002"; CEI Corporate Instruction CEI CI-211, "Protection of Personally Identifiable Information (PII)"; and, if

applicable, with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards.

4.7 Change Management

- Change Management procedure for IT managed systems can be found at the following link: IT Managed Systems
- Change Management procedure for non-IT managed systems can be found at the following link: Non-IT Managed Systems

5.0 RESPONSIBILITIES -- Both the sponsoring organization for the project and the IT organization are responsible for the deployment and support of new and existing information technology solutions. The two organizations have shared ownership of the project. Note: IT can also be the sponsoring organization.

5.1 IT approval is required prior to the selection or deployment of any information technology. Business organizations are required to contact the IT organization to discuss IT projects and obtain approval, see IT Project Registration Procedure for more information.

5.2 The responsible parties must establish a project steering committee for any project in excess of $20 million and/or projects requiring a steering committee.

6.0 REFERENCES –

6.1 GAP-911C: Accounting for Software Costs

6.2 GAP-960C: Accounting for Website Development Costs

6.3 IT Project Waterfall Playbook

6.4 IT Project Agile Playbook

6.5 CREATe - IT Project Registration Procedure

6.6 IT Capital Project Management Procedure

6.7 IT Project Management Guide

6.8 SDLC Guide

7.0 ADVICE AND COUNSEL -- CECONY's Vice President of IT Engineering and Operations and Vice President of IT Solutions Delivery shall provide advice and counsel on this Instruction.

8.0 **POLICY OWNER** – Vice President of IT Engineering and Operations

9.0 **REVIEW CYCLE** – This corporate policy is reviewed every five years.

10.0 **SUMMARY OF CHANGES** –

APPROVED DATE	SUMMARY OF CHANGES
September 30, 2024	• Section 4.2 (b) – Added to include instructions for CET • Section 4.7 – Added a new section for Change Management for IT Managed and Non-IT Managed systems. • Updated hyperlink for 6.5 and removed '6.8 – IT Application Roadmap Procedure' • Section 8.0 – Updated Policy Owner
April 28, 2023	This document was updated to incorporate changes related to new and updated IT procedures and guides, specifically related to the management of IT capital projects. The changes include updates of in the Applicability, Definitions, Procedure, References and Advice and counsel sections. A RACI chart that was part of the Exhibits was removed.

Software Development Lifecycle (SDLC) Guide

Version 5.0 • 01 – 01 – 2026



CREATED BY ETS PMO – V5.0 – Release Date: 12-26-2025 – Effective Date: 01-01-2026

CONTENTS

Section 1. Overview 4
Purpose 4
Development methodologies 4
Applicability and Governance 4
Tailoring this guide: 4
Artificial Intelligence (AI) Responsible Use Guidelines 4
SDLC Phases Breakdown 5
Definitions 6
Section 2. Responsible, Accountable, Consulted, and InformED Matrix (RACI Matrix) 16
Section 3. SDLC Quality Assurance 23
Project Documentation Repository Requirements 23
Project Status Reporting 23
Section 4. SDLC Project Phases 24
Phase 0: Preliminary and Project Overview 24
Phase Activity: Preliminary Design 24
Phase Activity: Pre-implementation Planning 29
Phase Activity: Value Realization Management 32
Phase Activity: Phase 0 Entry/Exit Criteria 33
Phase 1: Envision 34
Phase Activity: Initiation 34
Phase Meetings 39
Phase Activity: Envision Entry/Exit Criteria 40
Phase 2: Plan 41
Phase Activity: Planning 41
Phase Activity: Requirements Gathering 46
Phase Meetings 49
Phase Activity: Plan Entry/Exit Criteria 51
Phase 3: Build 52
Phase Activity: Design & Development 52
Phase Meetings 56
Phase Activity: Build Entry/Exit Criteria 57
Phase 4: Test 58
Phase Activity: System Testing 58
Phase Activity: Testing Strategy and Execution 59

Phase Meetings 60
Phase Activity: Test Entry/Exit Criteria 61
Phase 5: Deploy 66
Phase Activity: Pre-Deployment 66
Phase Activity: Post Deployment 67
Phase Activity: Hypercare 68
Phase Activity: Project Closure 71
Phase Meetings 73
Phase Activity: Deploy Entry/Exit Criteria 74
Section 5. SDLC Guide Document Change Management 75

SECTION 1. OVERVIEW

Any references to Information Technology (IT) in this document pertains to the newly branded organization of Enterprise Technology & Security (ETS).

PURPOSE

This SDLC Guide provides a standardized framework for executing technology projects governed by CEI-215 Corporate Instruction Acquisition Deployment and Support of Enterprise Technology and Security. The guide supports consistent quality, effective risk management, and project outcomes that meet defined acceptance criteria across Con Edison technology implementations.

DEVELOPMENT METHODOLOGIES

Project Managers are responsible for selecting the appropriate development methodology for their project (Waterfall, Agile, Hybrid). This guide accommodates various methodologies while maintaining consistent governance and deliverables. This guide outlines standard lifecycle phases. Teams using Agile or iterative methodologies may execute phases concurrently or cyclically, provided key control gates (Security, UAT, Production Approval) are completed as defined.

APPLICABILITY AND GOVERNANCE

This guide is required for all technology projects, whether managed by ETS or the business, unless an exception is granted by ETS leadership. Alternative methodologies are expected to demonstrate governance, quality controls, and deliverables equivalent to those defined in this guide. Vendors and contractors:

External vendors and contractors are responsible for following this guide or demonstrating equivalent governance and quality controls through their own methodology. Specific requirements are documented in the Statement of Work (SOW) and contract terms.

TAILORING THIS GUIDE:

Project teams may tailor this guide based on project size, complexity, and risk while maintaining required deliverables and governance requirements. Alternative approaches require ETS leadership approval. Contact the ETS PMO for tailoring guidance.

ARTIFICIAL INTELLIGENCE (AI) RESPONSIBLE USE GUIDELINES

Project team members should comply with Con Edison's AI Responsible Use Guidelines when using AI tools throughout the SDLC for activities such as requirements analysis, code generation, testing, documentation, and project planning.

SDLC PHASES BREAKDOWN

Phase 0 is required only for projects exceeding $20 million in total capital costs. Projects under $20 million may begin with the Envision Phase.

Phase Name	Phase Activity
0. Phase 0*	Preliminary Design
	Pre-implementation Planning
	Value Realization Management
1. Envision	Initiation
2. Plan	Planning
	Requirements Gathering
3. Build	Design & Development
	Unit Testing
4. Test	System Testing
	User Acceptance Test (UAT)
5. Deploy	Pre-Deployment
	Post Deployment
	Hypercare
	Project Closure

* NOTE: Phase 0 is required for projects exceeding $20 million in total capital cost.

DEFINITIONS

RACI Matrix

RACI Code	Definition
Responsible (R)	The person assigned to do the work to complete the task or activity.
Accountable (A)	The person who approves the completed work and has final decision authority. Only one person should be Accountable for each activity unless marked with an asterisk (*) indicating joint accountability.
Consulted (C)	The person whose input and expertise are needed before the task or activity is complete. Two-way communication.
Informed (I)	The person who is kept updated on the progress and completion of the task or activity. One-way communication.

Project Roles

Role	Description
Business Executive (Business Sponsor)	The Business Executive is accountable for project success and business value delivery. This person approves the project charter, business requirements, and production go-live. The Business Executive supports the project alignment with business strategy and delivers expected benefits.
Business Lead	The Business Lead is the day-to-day business leader responsible for business outcomes and deliverables. This person manages the business team, defines requirements, conducts User Acceptance Testing, and validates that the solution meets business needs. The Business Lead may serve as the Project Manager for business-led projects.
Backout	A documented procedure to reverse changes made during deployment and restore the system to its previous state. Used when issues found during production deployment cannot be fixed without rolling back.
ETS Executive	The ETS Executive approves the technical approach, ETS resource commitments, and financial governance decisions. This person is accountable for all technical activities, technical decisions, project planning, budget management, and scope control.

ETS Lead	The day-to-day technical leader responsible for technical delivery. This person manages development teams, infrastructure activities, technical design, testing, and deployment. The ETS Lead creates technical deliverables, validates technical quality, and is accountable for adherence to this SDLC Guide.
Project Manager (PM)	The person who manages project execution including schedule, budget, risks, issues, vendor coordination, and stakeholder communication. The Project Manager verifies SDLC compliance and reports project status to both Business Lead and ETS Lead. The Project Manager role may be filled by the Business Lead, Systems Manager, or a dedicated project management resource.

Terminology

Term	Definition
Agile	An iterative project methodology where requirements and solutions evolve through collaboration between cross-functional teams. Agile delivers working software in short cycles (sprints) with frequent feedback.
API (Application Programming Interface)	A set of protocols and tools that allow different software applications to communicate with each other. APIs enable real-time data exchange and system integration.
Application	The software system that implements the solution. The application is one component of the overall solution.
Baseline	An approved version of a project deliverable (such as requirements, design, or project plan) that can only be changed through formal change control procedures. The baseline serves as the reference point for measuring project progress and changes.
Baseline Version	An approved version that serves as the official reference. Changes to baseline versions require formal approval.
Business Requirements Document (BRD)	A document created by the Business Lead that describes what the system are expected to do from a business perspective. The BRD includes business processes, functional requirements, business rules, user roles, and acceptance criteria.
Capital Project	A project where costs are capitalized (recorded as assets) rather than expensed. Capital projects typically involve acquiring, building, or significantly enhancing systems or infrastructure with useful life exceeding one year.

Change Agent	A person who champions the change, influences others to adopt the new system, and helps overcome resistance. Change agents are typically respected business users who embrace the change.
Cloud Computing	Delivery of computing services (servers, storage, databases, networking, software) over the internet rather than on-premises infrastructure. Cloud deployment models include public cloud, private cloud, and hybrid cloud.
Commercial Off-The-Shelf (COTS)	Pre-built software purchased from a vendor rather than custom-developed. COTS software is configured to meet business needs rather than built from scratch.
Conference Room Pilot (CRP)	A working session where the development team demonstrates configured functionality to business users to validate design decisions and gather feedback before formal testing begins. Also called a design workshop or prototype review.
CREATe (Corporate Request for Evaluation and Approval of Technology)	Con Edison's technology governance process that requires projects to obtain approval from six review teams: Architecture, Security, Infrastructure, Integration, Data, and Compliance.
Current Working Estimate (CWE)	The project's current budget forecast includes all approved changes. The CWE is updated throughout the project lifecycle as scope, schedule, or costs change.
Cutover	The process of transitioning from the old system to the new system, including final data conversion, production deployment, and user transition activities.
Cybersecurity	The practice of protecting systems, networks, and data from digital attacks, unauthorized access, and damage. Cybersecurity includes technical controls, policies, and procedures.
Data Conversion/Migration	The process of extracting data from legacy systems, transforming it to match the new system's data structure, and loading it into the new system. It is also called ETL (Extract, Transform, Load).
Defect Severity 1 (Critical)	A defect that causes system unavailability, data corruption, security breach, or loss of Priority 1 business functionality. Response time: Immediate (24/7).
Defect Severity 2 (High)	Major functionality is broken with significant business impact and no acceptable workaround. Response time: Within 4 business hours. Examples: Key features not

	working, incorrect calculations, major performance degradation, and significant user population affected.
Defect Severity 3 (Medium)	A defect where functionality is impaired with moderate business impact, but a workaround is available. Response time: Within 2 business days. Examples: Minor features not working, inconvenient workflow, limited user population affected, acceptable workaround exists.
Defect Severity 4 (Low)	A minor issue, cosmetic defect, or enhancement request with minimal business impact. Response time: Planned maintenance cycle. Examples: Spelling errors, formatting issues, minor usability improvements, nice-to-have features.
DevOps	A set of practices that combines software development (Dev) and IT operations (Ops) to shorten development cycles, increase deployment frequency, and improve reliability through automation and collaboration.
Edge Systems	Applications or systems that send data to or receive data from the application being implemented. Edge systems may also be referred to as interfacing systems or integrated systems.
FERC (Federal Energy Regulatory Commission)	Federal agency that regulates interstate transmission of electricity, natural gas, and oil. FERC establishes rules and regulations that utility companies are expected to follow.
Go-live	The event when the application is deployed to production and becomes available for business use. Also called production deployment or cutover.
Hypercare	An enhanced support period immediately following production deployment, typically lasting 4-12 weeks, where the project team provides intensive support to resolve issues, optimizes performance, and supports user adoption.
Hybrid Methodology	A project approach that combines elements of Waterfall and Agile methodologies. For example, using Waterfall for planning and governance while using Agile for development and testing.
Interface/Integration	A connection between two systems that enables automated data exchange. Interfaces can be real-time (synchronous) or batch (scheduled file transfers).
Job Aid	A quick reference guide that provides step-by-step instructions for specific tasks or processes. Job aids are used at the point of work to support users.

Major Version	A significant update that includes substantial changes, new features, or revised processes. For major versions increase the first number (e.g., 1.0 to 2.0).
Managed Service Provider (MSP)	The company that provides ongoing application support, maintenance, and enhancement services after production deployment.
Middleware	Software that connects different applications or system components, enabling them to communicate and exchange data. Common middleware includes message queues, API gateways, and integration platforms.
Minor Version	A small update that includes corrections, clarifications, or minor enhancements. Minor versions generally increase the second number (e.g., 2.0 to 2.1).
NERC (North American Electric Reliability Corporation)	Organization that develops and enforces reliability standards for the bulk power system in North America. NERC standards include cybersecurity requirements (CIP standards).
Non-Production Environments	Environments used for development, testing, and training that are separate from the production environment. Common non-production environments include Development (DEV), System Integration Testing (SIT), User Acceptance Testing (UAT), and Training.
On-premises	Applications and infrastructure hosted and maintained within Con Edison's own data centers rather than in the cloud.
Operations & Maintenance (O&M)	Ongoing costs to operate and maintain systems after production deployment. O&M costs are expensed rather than capitalized.
Organizational Change Management (OCM)	A structured approach to transitioning individuals, teams, and the organization from current state to future state. OCM includes stakeholder engagement, communication, training, and adoption activities to support successful system implementation.
Parallel Project	A separate project or initiative that shares dependencies, resources, or timelines with the current project. Parallel projects require coordination to manage shared constraints and risks.
Parallel Testing	Test(s) comparing results from the new system with results from the current production system using the same input data to verify accuracy and completeness.

Penetration Testing	Penetration testing is an authorized simulated cyberattack on a system to identify vulnerabilities that could be exploited by malicious actors. Also called pen testing or ethical hacking.
Performance Testing	Performance testing measures application response time, throughput, resource utilization, and scalability under expected and peak load conditions. Performance testing includes load testing, stress testing, and endurance testing.
Personal Identifiable Information (PII)	Information that can be used to identify a specific individual, such as name, Social Security number, address, phone number, email address, or financial account numbers. PII requires special protection under data privacy regulations.
PI360	Con Edison's project portfolio management system used to track project information, status, financials, and milestones.
POET (Project Order Estimate Total)	The project account number used to charge project costs. The POET is obtained through the Appropriation process.
Production Environment	The live operational environment where end users access the application to conduct business activities. Also called the production system or prod environment.
Project Charter	A document created by the Project Manager and approved by the Business Sponsor that formally authorizes the project. The charter defines project goals, scope, success criteria, high-level timeline, budget, stakeholders, and risks.
Project Status Report (PSR)	A monthly report generated in PI360 that summarizes project accomplishments, schedule status, budget status, risks, and issues.
Quality Assurance (QA) Review	A review conducted by the Portfolio Liaison to verify that the project is following the SDLC process, completing required deliverables, and maintaining appropriate documentation.
Regression Testing	Testing conducted after defect fixes or changes to verify that fixes did not break existing functionality.
Request for Proposal (RFP)	A formal procurement document issued to potential vendors requesting proposals for providing products or services. The RFP describes requirements, evaluation criteria, and contract terms.

Requirements Traceability Matrix (RTM)	A document that maps business requirements to corresponding design elements, test cases, and defects. The RTM verifies requirements are addressed and tested.
Return on Investment (ROI)	A financial metric that compares the net benefits (benefits minus costs) to the total costs. ROI is expressed as a percentage or ratio.
RICEW Object Catalog	An inventory of custom development objects including Reports, Integrations, Conversions, Extensions/Customizations, and Workflows. The RICEW catalog documents each object's purpose, complexity, and estimated effort.
Rollback	The process of reverting to the previous system version if the production deployment fails or encounters critical issues. The rollback plan defines procedures to restore the prior system state.
Sarbanes-Oxley (SOX)	Federal legislation establishes requirements for financial reporting, internal controls, and auditing. SOX-relevant applications require specific controls and audit trails.
Scope Creep	Uncontrolled expansion of project scope without corresponding adjustments to schedule, budget, and resources. Scope creep occurs when new requirements are added without following the formal change control process.
Scrum	A specific Agile framework that uses fixed-length iterations (sprints), daily stand-up meetings, sprint planning, sprint reviews, and retrospectives.
Security Testing	Testing to identify vulnerabilities, verify security controls, validate data protections, and confirm prevention of unauthorized access. Security testing includes vulnerability scanning, penetration testing, and security code analysis.
Service Level Agreement (SLA)	A contract provision that defines expected service levels including availability targets (uptime), performance targets (response time), support availability (hours of coverage), and incident response times.
Smoke Testing	Basic verification testing to validate that critical functionality works before proceeding with thorough testing. Smoke testing answers the question: "Does the system work well enough to proceed with detailed testing?"
Software as a Service (SaaS)	Cloud-based software accessed via subscription where the vendor hosts and maintains the application infrastructure. Users access SaaS applications through web browsers.

Software Vendor	The company that provides commercial off-the-shelf (COTS) software or Software as a Service (SaaS) application.
Solution	The overall business capability being delivered by the project, including people, process, technology, and organizational change components.
Sprint	A fixed time period (typically 2-4 weeks) in Agile methodology during which the team completes a defined set of work and delivers working functionality.
Stakeholder	Any person, group, or organization that is impacted by the project or can influence project outcomes. Stakeholders include end users, business sponsors, executives, support teams, and external parties.
Statement of Work (SOW)	A contract document that defines the scope of work, deliverables, timeline, responsibilities, and acceptance criteria for vendor services.
System Integration Testing (SIT)	Testing conducted to verify that the application correctly integrates and exchanges data with all interfacing systems (edge systems).
System Integrator (SI)	The third-party company contracted to implement and integrate the software solution, configure the application, conduct testing, and provide implementation services.
System Testing	Thorough testing conducted by the project QA team to verify that all application components work together correctly and meet functional requirements.
Technical Design Document	A document created by the ETS Lead that describes how the system will be built from a technical perspective. The Technical Design includes system architecture, infrastructure design, integration design, data design, and security design.
Total Cost of Ownership (TCO)	The thorough cost of a solution includes initial capital costs (implementation) and ongoing O&M costs (support, maintenance, licenses, infrastructure) over the solution's expected lifetime.
Training	Structured learning activities that teach users how to use the new system. Training includes instructor-led sessions, self-paced e-learning, job aids, and reference documentation.

Unit Testing	Testing conducted by developers to verify that individual code components (functions, methods, classes) work correctly in isolation.
User Acceptance Testing (UAT)	Testing conducted by business users to validate that the application meets business requirements and is ready for production use.
Version	A specific iteration of a document or system identified by a version number (e.g., 1.0, 2.0, 2.1).
Vulnerability	A weakness in a system, application, or process that could be exploited to cause harm. Vulnerabilities may be technical (software bugs, misconfigurations) or procedural (weak passwords, lack of training).
Warranty Period	A period following Hypercare, typically 90 days, where the System Integrator (SI) provides defect support under contract terms before transitioning to the long-term support model.
Waterfall	A sequential project methodology where each phase (requirements, design, build, test, deploy) is completed before the next phase begins. Waterfall is appropriate for projects with stable, well-defined requirements.

Abbreviations and Acronyms

RACI Code	Definition
API	Application Programming Interface
BRD	Business Requirements Document
CEI	Corporate Enterprise Instruction
COTS	Commercial Off-The-Shelf
CREATe	Corporate Request for Evaluation and Approval of Technology
CRP	Conference Room Pilot
CWE	Current Working Estimate
DevOps	Development and Operations
DR	Disaster Recovery
ETS	Enterprise Technology & Security (formerly Enterprise Technology and Security)
ETL	Extract, Transform, Load
FERC	Federal Energy Regulatory Commission
MSP	Managed Service Provider

NERC	North American Electric Reliability Corporation
O&M	Operations & Maintenance
OCM	Organizational Change Management
PII	Personal Identifiable Information
PIR	Post-Implementation Review
PM	Project Manager
POET	Project Order Estimate Total
PSR	Project Status Report
QA	Quality Assurance
RACI	Responsible, Accountable, Consulted, Informed
RAID	Risks, Assumptions, Issues, Decisions
RFP	Request for Proposal
RICEW	Reports, Integrations, Conversions, Extensions, Workflows
ROI	Return on Investment
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RTM	Requirements Traceability Matrix
SaaS	Software as a Service
SDLC	Software Development Lifecycle
SI	System Integrator
SIT	System Integration Testing
SLA	Service Level Agreement
SME	Subject Matter Expert
SOW	Statement of Work
SOX	Sarbanes-Oxley Act
TCO	Total Cost of Ownership
UAT	User Acceptance Testing
VRM	Value Realization Management

SECTION 2. RESPONSIBLE, ACCOUNTABLE, CONSULTED, AND INFORMED MATRIX (RACI MATRIX)

The RACI Matrix below provides high-level responsibility assignments for project activities across all phases. Each RACI activity may encompass multiple detailed tasks, templates, and deliverables documented in the phase-specific sections (Phase 0 through Phase 5). For complete task lists, required documents, and detailed guidance refer to the corresponding phase sections.

#	Phase	Activity	Business Executive (Project Sponsor)	Business Lead	ETS Executive	ETS Lead
1	Phase 0	Establish cross-functional team and steering committee	A	C	A	R
2	Phase 0	Establish and train Steering Committee	A	C	A	R
3	Phase 0	Create business case	A	R	C	C
4	Phase 0	Conduct fit/gap analysis	C	R	A	R
5	Phase 0	Create RICEW object catalog	C	R	A	R
6	Phase 0	Develop cost estimate using Capital Project Cost Estimator	C	R	A	R
7	Phase 0	Develop implementation options and approach	C	C	A	R
8	Phase 0	Select software vendor and system integrator	A	R	A	R
9	Phase 0	Create Request for Proposal (RFP) & Statement of Work (SOW)	A	R	A	R
10	Phase 0	Negotiate and execute vendor contracts	A	R	A	R
11	Phase 0	Secure capital funding approval and obtain POET	C	C	A	R
12	Phase 0	Determine if Value Realization Management (VRM) is needed	A	R	C	C

13	Phase 0	Develop high-level project plan for Phase 1	C	C	A	R
R – Responsible | A – Accountable | C – Consulted | I – Informed						
#	**Phase**	**Activity**	**Business Executive (Project Sponsor)**	**Business Lead**	**ETS Executive**	**ETS Lead**
1	Envision	Create and approve Project Charter	A	C	C	R
2	Envision	Complete CREATe registration	C	C	A	R
3	Envision	Complete SOX review (if SOX application)	C	C	A	R
4	Envision	Create PI360 entry	C	C	A	R
5	Envision	Establish ETS Project Repository	C	C	A	R
6	Envision	Create and maintain Project Plan	C	C	A	R
7	Envision	Create and maintain Project Team and Stakeholder List	C	C	C	R
8	Envision	Create and maintain Project Risks Log	C	C	A	R
9	Envision	Create and maintain Issues List	C	C	A	R
10	Envision	Complete Cyber Security Checklist	C	C	A	R
11	Envision	Develop cost estimate	C	R	A	R
12	Envision	Secure funding approval and obtain POET	C	C	A	R
13	Envision	Select vendors and execute contracts	A	R	A	R

14	Envision	Establish Scope Change Request Process	C	C	A	R
15	Envision	Submit monthly Project Status Reports (PSR)	I	C	I	R
16	Envision	Create Business Requirements Document (BRD)	C	R	C	C
17	Envision	Conduct stakeholder analysis and impact assessment	C	R	C	C

R – Responsible | A – Accountable | C – Consulted | I – Informed

#	Phase	Activity	Business Executive (Project Sponsor)	Business Lead	ETS Executive	ETS Lead
1	Plan	Approve Functional Requirements	A	R	C	C
2	Plan	Create Technical Design Document	C	C	A	R
3	Plan	Approve Technical Design	C	C	A	C
4	Plan	Create Infrastructure Strategy	C	C	A	R
5	Plan	Create Integration Architecture	C	C	A	R
6	Plan	Create Data Conversion Strategy and Plan (if data conversion needed)	C	R	A	R
7	Plan	Complete all six CREATe reviews	C	C	A	R
8	Plan	Obtain Architecture Review Board approval	C	C	A	R
9	Plan	Create and baseline Project Plan	C	C	A	R
10	Plan	Create System Test Plan	C	C	A	R

11	Plan	Create Organizational Change Management (OCM) Plan	A	R	C	C
12	Plan	Develop communication plan and strategy	A	R	C	C
13	Plan	Develop training strategy and materials	A	R	C	C
14	Plan	Create Deployment Plan	C	C	A	R
15	Plan	Define post-production support model	C	R	A	R
16	Plan	Manage vendor contracts and performance	C	C	A	R
R – Responsible | A – Accountable | C – Consulted | I – Informed						
#	**Phase**	**Activity**	**Business Executive (Project Sponsor)**	**Business Lead**	**ETS Executive**	**ETS Lead**
1	Build	Complete Readiness to Build Checklist	C	C	A	R
2	Build	Conduct technical development and configuration	C	C	A	R
3	Build	Conduct Conference Room Pilots (CRPs) with business users	C	R	C	R
4	Build	Conduct unit testing	C	C	A	R
5	Build	Execute Organizational Change Management (OCM) activities	A	R	C	C
6	Build	Manage scope change requests	C	C	A	R
7	Build	Submit application and cyber security design changes for approval	C	C	A	R

8	Build	Execute mock data conversions and business validation	C	R	A	R
R – Responsible | A – Accountable | C – Consulted | I – Informed						
#	**Phase**	**Activity**	**Business Executive (Project Sponsor)**	**Business Lead**	**ETS Executive**	**ETS Lead**
1	Test	Conduct System Testing	C	C	A	R
2	Test	Conduct System Integration Testing (SIT)	C	C	A	R
3	Test	Conduct Performance Testing	C	C	A	R
4	Test	Conduct Security Testing	C	C	A	R
5	Test	Create Requirements Traceability Matrix (RTM)	C	C	C	R
6	Test	Define User Acceptance Criteria	A	R	C	C
7	Test	Conduct User Acceptance Testing (UAT)	C	R	C	C
8	Test	Conduct Parallel Testing (if applicable)	C	R	C	R
9	Test	Manage and resolve defects	C	C	A	R
10	Test	Approve UAT results	A	R	C	C
11	Test	Deliver user training	C	R	C	C
12	Test	Measure training effectiveness and user readiness	C	R	C	C
13	Test	Create user documentation and job aids	C	R	C	C

14	Test	Approve production go/no-go decision	A	R	A	R
15	Test	Conduct UAT Go/No-Go decision meeting	A	R	A	R
R – Responsible | A – Accountable | C – Consulted | I – Informed						
#	**Phase**	**Activity**	**Business Executive (Project Sponsor)**	**Business Lead**	**ETS Executive**	**ETS Lead**
1	Deploy	Complete Production Readiness Review	C	C	A	R
2	Deploy	Conduct Production Go/No-Go decision meeting	A	R	A	R
3	Deploy	Create and execute Go-live production checklist and deployment plan	C	C	A	R
4	Deploy	Approve final authorization to move to production	A	C	A	C
5	Deploy	Execute production deployment	C	C	A	R
6	Deploy	Execute production data conversion and validation	C	R	A	R
7	Deploy	Conduct production verification testing	C	C	A	R
8	Deploy	Provide Hypercare support	C	R	C	R
9	Deploy	Track user adoption metrics and execute sustainment plan	C	R	C	C
10	Deploy	Manage post-production defects and issues	C	C	A	R
11	Deploy	Execute transition to operations support team	C	C	A	R
12	Deploy	Create knowledge transfer documentation	C	C	A	R

13	Deploy	Conduct Post-Implementation Review (PIR)	A	C	C	R
14	Deploy	Document and share lessons learned	C	C	C	R
15	Deploy	Archive project documentation in ETS Project Repository	C	C	A	R
16	Deploy	Complete Legacy Application Retirement Plan (if applicable)	C	R	A	R

SECTION 3. SDLC QUALITY ASSURANCE

Active projects following the SDLC process undergo quality assurance reviews throughout the project lifecycle to confirm SDLC compliance and deliverable completeness. Quality assurance activities include:

- Conducting phase gate reviews at major milestones
- Verifying required deliverables and approvals
- Assessing project health (schedule, budget, risks)
- Verifying compliance with Con Edison standards and procedures

PROJECT DOCUMENTATION REPOSITORY REQUIREMENTS

ETS projects are expected to maintain documentation in the ETS Project Library. This includes key documents, project logs, and approvals. The ETS Project Library provides consistent, accessible documentation storage for in-scope projects.

To establish a project workspace, the Project Manager submits the official request form at ETS Project Library Request . Upon submission, the requester receives an email confirmation and a link to the automatically created project folder containing templates that can be used as needed and tailored for the project. All templates referenced in this guide are available in the ETS Project Library.

PROJECT STATUS REPORTING

Projects are expected to provide monthly status updates to maintain visibility and accountability. Quarterly reporting to appropriate governance bodies may be required based on project size and strategic importance. The Project Manager submits status reports to the Business Sponsor, ETS Executive, and ETS PMO. Status reports should be generated in PI360 or other approved project management tools and uploaded to the ETS Project Library.

SECTION 4. SDLC PROJECT PHASES

The following section describes each project phase, the documents needed, their usage, and required actions.

SDLC PHASE OVERVIEW

PHASE 0: PRELIMINARY AND PROJECT OVERVIEW

Phase 0 is required for projects exceeding $20 million in total capital costs and may be beneficial for complex initiatives regardless of cost.

Completing Phase 0 establishes the foundation for proper governance and team alignment. If Phase 0 deliverables are incomplete, projects may experience risks including missed requirements, vendor misalignment, cost overruns, and schedule delays.

PHASE ACTIVITY: PRELIMINARY DESIGN

This activity focuses on assessing project feasibility through requirements gathering, solution evaluation, and business case development. The cross-functional team conducts detailed analysis to determine whether the project should proceed to implementation.

Task	Documents / Steps	More Information
Establish Cross-functional Team	☐ Form cross-functional team **(Required)**	**Cross Functional Team**: *Cross-Functional Team: Form a dedicated cross-functional team with appropriate representation from business and ETS. Train the cross-functional team on the proposed solution(s).* *Team composition should reflect the scope and complexity of the solution. Include business SMEs to define requirements and ETS resources to assess technical feasibility, architecture, and integration requirements.*
Create Cross-functional Steering Committee	☐ Establish Steering Committee **(Required)**	*Establish a Steering Committee composed of General Managers and Vice Presidents to provide strategic guidance and oversight throughout Phase 0.* *Define the committee's composition, meeting cadence, decision-making authority, and escalation paths.* *This committee plays a critical role in reviewing deliverables, making key decisions, and ensuring alignment with organizational priorities.*

Task	Documents / Steps	More Information
Train Key Stakeholders on SDLC	☐ Educate Steering Committee on SDLC	***Steering Committee:*** *All Steering Committee members are expected to be educated in SDLC, RACI, and the project's scope.*
Coordinate Phase 0 Funding Strategy	☐ Coordinate with Cost Management and Accounting	**Funding Estimates:** *Coordinate with Cost Management and Accounting to establish appropriate account structures. Funding estimates should account for the size of the cross-functional team and the expected duration of Phase 0 activities. If the project does not proceed, Phase 0 costs typically revert to O&M. If approved for implementation, costs transfer to capital accounts. Discuss with Cost Management and Accounting at project initiation how long costs can remain in preliminary accounts before final classification.*
Determine Software Selection Approach	☐ Determine if software is pre-selected or to be identified	*Determine whether the software application has been pre-selected or needs to be identified during Phase 0. For pre-selected software, focus on detailed scope, cost estimates, timeline, and implementation options.* *If software is to be determined, dedicate the first several weeks to developing business requirements, creating a vendor short list, conducting demonstrations, and evaluating options. Pre-selected software allows for more robust cost estimating and implementation planning.* *When evaluating hosting options, cloud-based infrastructure is the default approach. On-premises hosting may be appropriate for systems with specific requirements such as real-time operational control, regulatory constraints, data sovereignty needs, or unique integration requirements. Any decision to deploy on-premises should be documented with clear technical and business justification.*
Identify Project SMEs / Key Resources	☐ Identify and secure SMEs	*Identify and secure business and ETS subject matter experts needed for Phase 0. Work with HR regarding staffing needs, position postings, transition timelines, and backfill requirements. Key resources should be available and committed for the duration of Phase 0.*
Create Business Requirements & Use Cases	☐ Document business requirements and use cases **(Required)**	*Document thorough business requirements and use cases, including detailed scenarios and workflows that describe how the system will be used across different business processes and user roles. Determine and document business process flows and identify any organizational changes required.*

Task	Documents / Steps	More Information
		Identify training requirements, number of employees/roles to be trained, who will create training material and conduct the training. *Business requirements and use cases are expected to be documented and approved by business leadership.* *This forms the foundation for all subsequent Phase 0 deliverables.*
Conduct a Fit/Gap Analysis	☐ Conduct Fit/Gap analysis **(Required)**	**Fit/Gap Analysis –** *The cross-functional team evaluates how well the proposed software application meets business requirements. For each requirement, document whether the solution provides:* - *Fit: Meets requirement with standard functionality* - *Partial fit: Meets some but not all aspects* - *Gap: does not meet requirement.* *For critical gaps, evaluate whether customization is justified or if business processes can be adapted.* *See Fit/Gap Analysis Template to document findings. The fit/gap analysis directly informs the RICEW catalog and cost estimates.* *Conduct vendor demonstrations and document functional alignment using the fit/gap categories.* *Evaluate identified gaps to determine necessity and whether customization is justified or if business processes can be adapted. All identified gaps are expected to be reviewed in detail to determine if the functionality is truly required. For critical gaps, evaluate whether customization is justified or if an alternative solution should be considered.* *The fit/gap analysis directly informs the RICEW catalog and cost estimates. Finalize with stakeholder approval to confirm solution direction.*
Identify RICEW Catalog	☐ Create RICEW catalog **(Required)**	**RICEW Object Catalog** – *Identify all Reports, Interfaces, Conversions, Enhancements/Extensions, and Workflows required. For each RICEW object, document the business purpose, complexity (simple, medium, complex), estimated effort, technical approach, and dependencies. Focus on minimizing customizations and maximizing use of standard product capabilities.* *See RICEW Object Catalog Template to document all custom development objects. The RICEW catalog is a key input to cost estimates and implementation planning.*

Task	Documents / Steps	More Information
		- *Focus on minimizing customizations and maximizing use of standard product capabilities. The RICEW catalog is a key input to cost estimates and implementation planning. Business and ETS stakeholders should review and validate the catalog for completeness and accuracy.*
Develop Cost Estimate	☐ Use Capital Project Cost Estimator app **(Required)**	**<u>Capital Project Cost Estimator Application</u>** – *Use the app to develop detailed cost estimates including appropriate contingency based on project risk and uncertainty.* *The cost estimate should include capital costs: internal labor, SI labor, other vendors, external SME contractors, staff augmentation, software licensing, hardware, training, change management, facilities costs, contingency, and overhead. Document timeline with major SDLC activities (Analysis, Design, Build, Test, Training, Deploy), including estimated durations and resource requirements.* *Identify ongoing post-production O&M costs including business and ETS support labor, software maintenance fees, infrastructure costs, and planned upgrade costs over 3-5 years.* *Cash flow projections should align with the implementation timeline and account for payment schedules with vendors.* *Any significant facilities requirements (leasing additional space, renovating existing space, specialized infrastructure) should be identified with associated costs and timelines.* *Large projects (>$20M) should have a dedicated FPA resource to manage CWE and actuals throughout the project and report budget variances to the Steering Committee.*
Develop Implementation Options	☐ Evaluate implementation strategies	**<u>Implementation Options Analysis</u>** – *Define and evaluate implementation strategies such as big bang (implement across all areas simultaneously), phased deployment by division or region, or rollout by functional area (implement modules incrementally). For each option, document pros and cons, implementation timeline, resource requirements, cost implications, and risk considerations. Big bang minimizes dual-system support but carries higher risk. Phased deployment allows for learning between phases and reduces risk but extends timeline. See Implementation Options Analysis Template to structure the evaluation. The recommended approach should be clearly justified based on project-specific factors.* *Rollout by functional area implements modules incrementally. This approach provides early value but may create integration challenges. For each option,*

Task	Documents / Steps	More Information
		document pros and cons, implementation costs, timeline impacts, resource requirements, and risk considerations. The recommended approach should be clearly justified based on project-specific factors.
Develop Business Case	☐ Business Case Template **(Required)**	**<u>Business Case Template</u> –** *The business case justifies the project investment and provides the foundation for the go/no-go decision. The Business Lead creates the business case, which typically contains the following:* - *Business problem or opportunity* - *Proposed solution options* - *Cost-benefit analysis* - *Financial analysis (ROI, NPV, payback period)* - *Risk assessment* - *Implementation approach* *See Business Case Template for structure and required content.* *Some additional considerations:* *Benefits should be categorized and quantified:* - *FTE reductions: Identify specific positions, timing, and annual savings* - *Compliance benefits: Regulatory requirements met, penalties avoided* - *Risk reduction: Quantified risk mitigation* - *Revenue increases: Quantify with assumptions and timing* *Cost avoidance: Expenses not incurred due to new solution.* *Conduct financial review to assess return on investment, cost of capital, rate impacts, and other financial considerations.* *Capital costs (implementation) and O&M costs (post-production support) should be clearly separated and aligned with the cost estimate.* *Identify how both costs and benefits will be tracked during implementation and post-production, including responsible parties, reporting frequency, and success metrics.*
Conduct Risk Assessment	☐ Identify and assess project risks ☐ Review lessons learned and key	*Identify preliminary project risks including technical complexity, organizational change impact, vendor viability, integration challenges, resource constraints, and schedule dependencies.* *For each significant risk, assess likelihood and impact, and develop high-level mitigation strategies.*

Task	Documents / Steps	More Information
	risks from other relevant projects.	*Critical risks should be escalated to the Steering Committee and factored into implementation planning and contingency estimates.*
Define Governance Model	☐ Establish governance structure	*Establish the governance structure for implementation including Steering Committee composition, decision-making authority, escalation paths, and reporting cadence.* *Define roles and responsibilities using a RACI matrix.* *Address how changes will be managed, how issues will be escalated and resolved, and how progress will be monitored and reported.* *The governance model provides the framework for Phase 1 implementation oversight and accountability.*
Create RFP	☐ Draft Request for Proposal	*The Phase 0 internal team (Con Edison employees) is responsible for drafting the Request for Proposal (RFP) to support fairness and prevent conflicts of interest. If an SI is engaged during Phase 0, they should typically be excluded from bidding on Phase 1 implementation work to maintain independence and objectivity.* *The RFP should be structured to support the selection or procurement of:* - *Software vendor* - *System integrator* - *Business integrator* - *Project Management Office or Value Management Office* - *Organizational Change Management provider (including training)* *Conduct a review of past RFPs to incorporate pain/gain language and strategies for managing project costs and change requests.* *If the selected vendor is not on Con Edison's approved vendor list, allow adequate time for Terms and Conditions review and approval. This process may take 2-3 months and should be factored into project planning.* *The recommended practice is to avoid selecting the same vendor for both the solution and system integration (SI).*

PHASE ACTIVITY: PRE-IMPLEMENTATION PLANNING

This activity focuses on securing approvals, finalizing contracts, and preparing for Phase 1 implementation. Upon completion of preliminary design deliverables, the project team socializes results with stakeholders and executes procurement and planning activities necessary to launch implementation.

Task	Documents / Steps	More Information
Socialize Results	☐ Collect stakeholder feedback	*Collect and document feedback from each stakeholder group (Business Area VP and/or Lead, ETS VP, Purchasing GM/VP, Cost Management team). After collecting feedback, assess the impact and update the implementation plan and financial models accordingly.* *Secure necessary approvals and communicate changes to relevant teams.* *Feedback may require changes to the implementation plan, cash flow adjustments, internal FTE allocations, evaluation of alternative implementation options, or ROI refinements.*
Obtain Funding Approval	☐ Submit for funding approval **(Required)** ☐ Submit for Ruling Decision: Unifier Request **(Required)** ☐ Secure Funding: Portfolio Management Playbook **(Required)** ☐ Obtain Project Account POET: Appropriations Guide **(Required)**	*If the project is ruled as a capital project, funding needs to be requested through the appropriate governance body (IT Board).* *If the project cost estimate exceeds $75K, submit a ruling request via Unifier.* *Submit an appropriation for the project in Unifier to obtain a POET. A POET is the project account used to track and charge project costs.* *For guidance on Delegation of Authorities, please refer to Corporate Policy Statement 000-1 Delegation of Authorities.*
Identify Hardware / Software needed	☐ Order hardware and software	*Initiate procurement for all required hardware and software. Coordinate with Procurement and Infrastructure teams for ordering, delivery tracking, and installation scheduling.*

Task	Documents / Steps	More Information
	☐ Review Supply Chain Request (Software)	*Make decisions regarding server orders (or cloud provisioning), team location, and startup activities (desks, PCs, conference rooms, network IDs for SI/contractors).* *Order, download, and install all required applications and database software (e.g., Oracle, MQ, WebSphere, Maps).* *Infrastructure preparation supports Phase 1 to begin without delays.*
Prepare initial 90-day plan for Implementation	☐ Develop initial 90-day implementation plan	*Develop a detailed 90-day plan for Phase 1 initiation, including team formation, workspace preparation, and initial activities. The 90-day plan should outline immediate next steps and critical path activities for Phase 1 startup.*
Create and track Contracting / Requisition documentation	☐ Create and track contracting documentation ☐ Request for Proposal (RFP) Guide ☐ Statement of Work Template (SOW)	*Engage the Purchasing department to prepare requisitions and issue Requests for Proposal (RFPs) for System Integrator (SI) services and software solutions (if not already selected).* *Define the selection process in advance, including evaluation participants, scoring criteria, purchasing review requirements, and approval authorities.* *Following vendor selection, finalize the Statement of Work and Terms and Conditions.* *Request for Proposal (RFP) Guide – Supply Chain's process for vendor selection and contracting. Consider selecting a system integrator (SI) that is independent from the software vendor to avoid conflicts of interest and support objective implementation of the solution.* *Statement of Work Template (SOW) – The document should include:* - *Scope of the project - Which parts of the vision will be satisfied.* - *Out of Scope items – Areas not required for the project purposes.* - *The Project Business Requirements – the statement of business needs.* - *Deliverables List – All documents needed as part of the project.* - *Quality of service requirements, also known as Service Level Agreement or SLA, requirements that define expectations between the service provider and the service recipient. Be sure to record the criticality of the application and requirements for application availability, performance metrics, and support availability. Define the service level of the*

Task	Documents / Steps	More Information
		application and user needs from the perspective of availability, performance, and quality-of-service perspectives. *The SI contract should include appropriate T&Cs to protect against SI failures across all SI responsibilities, including defects management. It should also include SI termination criteria.*
Develop High Level Project Plan	☐ Create high-level project plan **(Required)**	*Finalize the initial project plan including major activities and tasks with an estimated schedule (start and end dates), risks, cost estimation, resources, and responsible parties.* *Finalize roles and responsibilities for both SI and internal teams (Business and ETS).* *Determine SI and business/ETS team composition. Establish procedures for adding or removing team members and backfilling when resources issues arise.* *This plan will be further refined as the project progresses. The project plan should be established in PI360 and/or MS Project.*
Review Cost Estimate	☐ Capital Project Cost Estimator app **(Required)**	*At the end of each phase of the SDLC, revisit the project cost estimate.*

PHASE ACTIVITY: VALUE REALIZATION MANAGEMENT

Value Realization Management (VRM) is a structured process applied throughout and after the implementation of transformational projects to identify, quantify, track, and report both financial and non-financial business benefits or stakeholder value delivered by the solution. A transformational project, as defined in the ETS Capital Project Management Procedure, is an initiative involving company applications that introduces significant changes to processes, technology, or organizational structures.

For transformational projects involving large-scale company applications that require Board approval as per CI-610-1 (> $50M), the project team should consider implementing a VRM process similar to the process outlined in the CORE Value Realization Management Repeatability Guide.

The project team has discretion to scale and tailor the VRM process to meet the needs of the project. If it is determined that a VRM process will be implemented, the project team is responsible for revisiting Phase 0 Deliverables to account for the additional scope, cost, and contractual elements required to implement this process.

If the Business Executive (i.e., Business Sponsor) determines VRM is not warranted, they should provide a justification. Ownership of the VRM process resides with the Business Executive and Business Lead as outlined in the RACI Matrix above.

Task	Documents / Steps	More Information
Make determination on Value Realization Management (VRM)	☐ CORE Value Realization Management Repeatability Guide	*The CORE Value Realization Management Repeatability Guide provides an example of a VRM framework that can be tailored and adopted by other projects.* *Transformational projects involving large-scale company applications that require Board approval under CI-610-1 should consider implementing a Value Realization Management (VRM) process similar to the process contained in the CORE Value Realization Management Repeatability Guide.*

PHASE ACTIVITY: PHASE 0 ENTRY/EXIT CRITERIA

Entrance	Exit
☐ Business need or opportunity identified and documented ☐ Executive sponsor committed to funding Phase 0 analysis ☐ Cross-functional team availability confirmed ☐ Phase 0 budget and timeline approved ☐ Business case development assigned to Business Lead	☐ Project has received a go or no-go decision from the Business Executive (Sponsor)* ☐ Initial funding secured through the Appropriation/Authorization process and POET Obtained ☐ Major contracts have been awarded or are in final negotiation ☐ High-level project plan has been developed and approved by key stakeholders ☐ Lessons learned documented and deliverables archived in the ETS Project Library for future reference. *Projects that are operationally required or regulatory mandated may need to proceed even if there are no proven financial benefits.

PHASE 1: ENVISION

PHASE ACTIVITY: INITIATION

The Envision phase focuses on high-level vision and scope for the project. Key inputs include resource identification from business and ETS, stakeholder identification, potential risks, high-level timeline, and budget with contingency. The Project Manager should complete all documents and obtain the needed approvals to continue pursuing the project. Approvals throughout this document may be email approval, meeting minutes, or formal document signature as appropriate for project governance.

Task	Documents / Steps	More Information
Review the ETS Capital Project Management Procedure	☐ ETS Capital Project Management Procedure **(Required)**	*The ETS Capital Project* Management *Procedure provides information on ETS Project Management practices and compliance requirements.*
Review CEI-407 Data Classification	☐ CEI-407 Data Classification **(Required)**	*The procedure provides information on protecting the restricted and confidential information of the Company or in the Company's possession by establishing a data classification policy.*

Task	Documents / Steps	More Information
Start CREATe (Corporate Request for Evaluation and Approval of Technology) Process	☐ ETS Project Registration Procedure (Link to Procedure)(CREATe App)**(Required)** **All items below are (Required):** ☐ Cyber Security Checklist ☐ Vendor Risk Assessment ☐ Third Party Software Evaluation ☐ Personal Identifiable Information (PII) ☐ Architecture Diagram	*CEI-215 requires technology projects to be registered with ETS for strategic alignment review and portfolio visibility. CREATe is a process for evaluation and approval as well as an application that facilitates collaboration and tracking. Follow the instructions within the CREATe system to begin submission and approval of the project.* **Cyber Security Checklist** – *The design should comply with published ETS guidance for application security and EA. The ETS Project Manager and/or Project Lead is to complete this checklist, which identifies areas of security concerns to determine if security gaps exist.* **Vendor Risk Assessment** – *This form is required if data will be transmitted. If the vendor is new, the vendor will get qualified during the Requisition process with Procurement. ETS approval should be received before proceeding with the Requestion Process.* *Check Qualified Vendors list to see if this is a new vendor: Qualified Supplier List* **Third Party Software Evaluation** – *This form is required if the project requires new software.* **Personal Identifiable Information** – *This form is required if personal data is involved in a project. CREATe sends PII/PIA Form once the PM indicates that a CREATe Request touches PII/PIA data.*

Task	Documents / Steps	More Information
Create PI 360 Project (Required for Capital Projects)	☐ PI 360 Link ☐ White Paper **(Required)** ☐ PI 360 Guide	***All capital projects*** *should be created in PI 360. Provide project information and financial details. Project teams are responsible for following SDLC phases to maintain project structure and consistency. ETS PMO reviews compliance at each phase. Strategic projects may require a cost benefits analysis, see CI 291-1 Cost Benefit Analysis (CBA) Guidelines.* *Note: PI 360 has an autogenerate feature where a user can fill out white paper details within the system rather than downloading the white paper MS Word document and later uploading the document.* *PI 360 has a template of the white paper available as needed.*
Develop Project Cost Estimate	☐Capital Project Cost Estimator app **(Required)**	**Capital Project Cost Estimator Application** – *Used to develop thorough cost estimates including appropriate contingency based on project risk and uncertainty. The cost estimate should include the following:* - *All capital costs (internal labor, SI labor, other vendors, external SME contractors, staff augmentation, software licensing, hardware, training, change management, facilities costs, contingency, and overhead).* - *Timeline with major SDLC activities (Analysis, Design, Build, Test, Training, Deploy) with estimated durations and resource requirements.* - *Ongoing post-production O&M costs including business and ETS support labor, software maintenance fees, infrastructure costs, and planned upgrade costs over 3-5 years.* - *Cash flow projections aligned with the implementation timeline and account for payment schedules with vendors.* - *Any significant facilities requirements (leasing additional space, renovating existing space, specialized infrastructure) along with associated costs and timelines.*
Submit for Ruling Decision	☐ Unifier Request **(Required)**	*If the project cost estimate exceeds $75K, submit a ruling request via Unifier.*
Secure Funding	☐ Portfolio Management Playbook	*If a project is ruled as a capital project, funding needs to be requested through the appropriate governance body (IT Board).*

Task	Documents / Steps	More Information
Obtain Project Account POET	☐ Appropriations Guide	*Submit an appropriation for the project in unifier to obtain a POET. A POET is the project's account to charge a budget affiliated with the project costs. For guidance on Delegation of Authorities, please refer to the Corporate Policy Statement.* *000-1 Delegation of Authorities*
Create Project Charter	☐ Project Charter Template **(Required Approval)** ☐ Project Issues, Risks & Assumptions Logs Template **(Required)**	**Project Charter Template** – *A project charter is a formal document that authorizes the project and provides the Project Manager with written authority to begin work. A project charter document describes a project to create a shared understanding of its goals, analysis, and resource requirements. The document should include:* *-Vision and Scope* *-Project Benefit Analysis* *-In scope and out of scope activities / Deliverables* *-Stakeholder List with defined role* *-High-level Resource Plan* *-High-level project timeline* *-High-level test plans* *-Budget Summary* *-Assumptions & Risk Assessment* *-External / Internal QA review plan and periodic audits* **Project Issues, Risks & Assumptions Logs Template** – *On-going document updated by the Project Manager to track issues, assumptions & risks impact, and status.*
Create and track Contracting / Requestion documentation	☐ Request for Proposal (RFP) Guide ☐ Statement of Work Template (SOW)	**Request for Proposal (RFP) Guide** – *Supply Chain's process: An optional artifact if project is bringing in vendors such as system integrators, software vendors, PMO vendor, business integrator vendor, and/or change management vendor.* **Statement of Work Template (SOW)** – *Document shall include:* - *Scope of the project - Which parts of the vision will be satisfied.* - *Out of Scope items – Areas not required for the project purposes.* - *The Project Business Requirements – the statement of business needs.* - *Deliverables List – All documents needed as a part of the project.* **Quality of service requirements (also known as Service Level Agreement or SLA) –** *Requirements that define expectations between the service provider and the service recipient. Be sure to record the criticality of the application and requirements for application availability, performance*

Task	Documents / Steps	More Information
		metrics, and support availability. Define the service level of the application and user needs from the perspective of availability, performance, and quality of service. *SI contracts should include the right Terms and Conditions (T&Cs) to protect against SI failures in all their responsibilities including defects management. It should also include SI termination criteria.*
Vendor On-boarding	☐ Vendor on-boarding Guide ☐ On-boarding Tracker Template	**Vendor on-boarding Guide** – *If there is a new vendor or new contractor resources utilized on the project, review the guide and share details with Vendor assigned employees.* **On-boarding Tracker Template** – *Document all names registered and onboarded into Con Edison systems. The document is useful for off-boarding when the project is completed.*
Create a Project Status Report	☐ PI360 Project Status Report **(Required)** ☐ Meeting Minutes Template	**PI360 Project Status Report (PSR) Guide**– *Use the PI360 PSR User Guide to generate a Project Status Report. Project Status Reports are required monthly and are used throughout the project to report status, accomplishments, milestones, risks and issues, and dependencies to business owners and stakeholders.* **Meeting Minutes Template** – *Document all project meetings including kickoff, status meetings, design reviews, steering committee meetings, and change control board meetings.*
Sox Review	☐ SOX PMO ☐ SOX SDLC Narrative **(Required if SOX Application)**	**SOX (Sarbanes Oxley) – Optional** – *Review project for compliance requirements established by Sarbanes-Oxley (SOX). The SOX review validates that business processes for the software development project meet specified auditing objectives.*
Review Cost Estimate	☐ Capital Project Cost Estimator app **(Required)**	*At the end of each phase of the SDLC, revisit the project cost estimate.*

Task	Documents / Steps	More Information
Current Working Estimate	☐ Current Working Estimate Template **(Required)**	**Current Working Estimate (CWE)** – *The Project Manager maintains the CWE throughout the project lifecycle. The CWE is the project's current budget forecast including all approved changes and is required for projects > $2.5M. The CWE is updated whenever scope, schedule, or costs change. The Project Manager reports CWE variance to the ETS and Business Executives monthly.*

PHASE MEETINGS

Task	Description
Conduct an internal Kick-off meeting	*Meeting held with identified internal stakeholders* to confirm alignment before engaging / onboarding selected vendors.* ☐ Create Internal Project Kick-off Presentation *Bring approved vendor(s) to train teams on solution.
Business Sponsor and Project Manager meet to review and approve documentation	*This meeting is to review key activities and documents and obtain Business Sponsor's approval of the project's charter and any other key documentation such as vendor contracts.*

PHASE ACTIVITY: ENVISION ENTRY/EXIT CRITERIA

Entrance	Exit
☐ Business need or opportunity identified and documented ☐ Executive sponsor committed to funding project ☐ Project team availability confirmed	☐ Project Charter approved by Business Sponsor (documented approval with signature) ☐ CREATe registration complete and initial reviews passed ☐ PI360 project entry created with accurate information ☐ ETS Project Repository established with folder structure ☐ Scope Definition and Validation Checklist complete ☐ Scope validated with key stakeholders and documented ☐ Scope baseline approved by Business Sponsor and ETS Executive (documented approval) ☐ High-level project plan created ☐ Cost estimate completed using Capital Project Cost Estimator app ☐ Cost estimate approved by ETS Lead ☐ Funding secured through IT Board (if capital project) ☐ POET obtained through appropriations process ☐ Vendors selected and contracts executed (if applicable) ☐ Change Control Plan established and approved ☐ Preliminary OCM Plan created ☐ All Envision Phase deliverables complete, approved, and archived in ETS Project Repository ☐ Business Sponsor and ETS Executive approve proceeding to Plan Phase

PHASE 2: PLAN

PHASE ACTIVITY: PLANNING

The Plan Phase is when the project team defines the detailed requirements, designs the technical solution, and plans all project activities. The Business Lead creates business requirements. The ETS Lead creates the technical design, infrastructure strategy, and integration architecture. The Project Manager develops and baselines the detailed project plan.

Task	Documents / Steps	More Information
Begin Documenting Legacy Application Retirement Plan	☐ Legacy Application Retirement Plan Template ☐ 870- 1 CI Records Management (sharepoint.com) **(Required)**	**Legacy Application Retirement Plan Template** – *Document handling the legacy application and retaining data.* *The Project Manager should keep in mind the cost of data retention.*
Order Hardware / Software	☐ Supply Chain Request (Software) ☐ Submit purchase requisitions ☐ Coordinate with Procurement team ☐ Track delivery timelines ☐ Coordinate with Infrastructure team for installation and configuration	*If any required hardware or software needs to be purchased, initiate procurement process.* *Make decisions regarding server orders (or cloud provisioning), team location, and startup activities (desks, PCs, conference rooms, network IDs for SI/contractors).* *Order, download, and install all required application and database software (i.e., Oracle, MQ, WebSphere, Maps, etc.).* *Infrastructure preparation increases the probability that the Build Phase can begin without delays.*

Task	Documents / Steps	More Information
Create a Change Control Plan	☐ Change Control Plan Template **(Required)** ☐ Scope Change Request Form Template	**Change Control Plan Template** – *This document articulates the project overview, governance structure, and the approach that will be used to execute the scope of work and manage changes that may occur during the project lifecycle.* **Scope Change Request Form Template** – *Each change is analyzed to determine the impact to the project in terms of schedule, budget, and risk. These scope change requests are then documented, and it is the business sponsor's decision whether to pursue the changes based on the analysis.* *Project governance is essential for effective scope management. The Change Control Board evaluates all scope changes against the project schedule and budget and approves them accordingly. Avoid scope creep. Collect and estimate day-2 items, identify and define them, and plan the approach for addressing them. Avoid adding unplanned project waves.*

Create Organization Change Management Plan	☐ Organizational Change Management (OCM) Template **(Required)**	**Organizational Change Management –** *The OCM Plan is required for projects that introduce significant changes to business processes, user roles, or system functionality. It describes the impact on end users and the organizational changes that will occur upon implementation. The OCM Plan includes:*
		
		- *Stakeholder Analysis:*
		  - *Stakeholder groups and impact assessment*
		  - *Engagement strategy by stakeholder group*
		- *Change Agent Network:*
		  - *Change agent identification by business area*
		  - *Change agent roles, training, and support plan*
		- *Resistance Management:*
		  - *Anticipated resistance points*
		  - *Mitigation strategies and escalation procedures*
		- *Adoption Metrics and Targets:*
		  - *User adoption rate targets (% users actively using system)*
		  - *Transaction volume targets*
		  - *User satisfaction targets*
		  - *Measurement approach and frequency*
		- *Communication Plan:*
		  - *Key messages by stakeholder group*
		  - *Communication channels and frequency*
		  - *Communication timeline by SDLC phase*
		- *Training Strategy:*

Task	Documents / Steps	More Information
		○ *Training approach by user role (instructor-led, e-learning, hands-on, job aids)* ○ *Training content outline* ○ *Training schedule and resources* ○ *Training effectiveness measurement* - *Reinforcement and Sustainment:* ○ *Post-go-live reinforcement activities* ○ *Ongoing support approach* ○ *Continuous improvement plan* *The Business Lead is responsible for OCM Plan creation and execution. OCM is not optional for transformational projects.* See OCM Plan Template for complete structure.
Identify Interdependencies	☐ PI 360 Job Aid – Creating Milestone Relationships and Dependencies	*Each parallel project should identify other projects or workstreams that could directly affect results or deadlines. These are tracked as dependencies. Dependencies can be tracked in PI360.* *Examples of Dependencies:* - *Hardware or Software Upgrades.* - *Major Enhancements such as Regulatory requirements, Account changes, Meter # changes, Emp # changes, etc. to the Edge or Interfacing Systems such as: improve monitoring, automation of manual processes, enhance business processes, hardware for either improving processing or capacity of environments that most likely will remain after the implementation of the Target Application is in. If this effort is deemed extensive, a separate capital project will need to be created and funded.* - *Technology obsolescence/ modernization.* - *Cyber Security requirements.*
Develop Detailed Project Plan	☐ Project Plan **(Required)**	*Include major activities and tasks with estimated schedule with start and end dates, risks, cost estimation, resources, and responsible parties.* *This plan will be further refined as the project progresses.* *Plan should be established in PI360 or MS Project.*

Task	Documents / Steps	More Information
Develop a Project team Registry	☐ Project team Registry Template **(Required)**	*The Project Manager can use the template to build project organization chart (team organizational structure) and track all responsible parties' details. The org chart is to include the steering committee for the projects over $10M and executives and audit reps in for the projects over $20M.* Verify that the project team includes SMEs from Technical (Infrastructure, Cyber Security) Functional Resources, and Business Resources.
Develop a Deployment Plan	☐ Deployment Plan Template **(Required)**	*The document's content should be collected throughout the project and finalized before production deployment.* *Project Transition Plan such as cut-over plan, Rollback (backout) plan, and Disaster Recovery Plan. The transition plan should include the handover to the RUN team.*
Define and approve support model budgets, contracts, licenses	☐ Capital Project Cost Estimator app **(Required)** ☐ RFP Guide and SOW Template ☐ Infrastructure and Middleware Strategy Documents ☐ License and Subscription Planning (referenced in Hypercare section) ☐ Monitoring Tools and Parameters (from Infrastructure Strategy)	*This task validates that the financial and contractual components of the long-term support model are proactively addressed during the planning phase. The Business Lead is responsible for identifying and documenting the estimated Capital and O&M budgets required to support the application post-deployment. This includes:* - *Forecasting costs for ongoing support contracts (e.g., MSP, vendor SLAs)* - *License and subscription requirements* - *Planning for production support labor and monitoring tools* - *Maintenance agreements and renewal timelines* *The Business Executive (Sponsor) is accountable for approving the support model and ensuring alignment with strategic and financial governance. ETS Executive and ETS Lead should be consulted to validate technical feasibility and operational readiness.* *This step aligns with CEI-215 requirements and supports that planning is not deferred to the Deploy phase but rather integrated into early project planning for better cost control and operational continuity.*

Task	Documents / Steps	More Information
Develop Meeting Schedule	☐ Meeting Schedules	*Examples of meeting schedules that can be planned based on the project methodology used are:* - *Weekly Status Review* - *Weekly RAID review* - *Weekly Change Control* - *Weekly Project Leadership Meeting* - *Monthly Resource Review* - *Monthly Budget Review* - *Monthly Steering Committee* - *Monthly Architecture Review Board* - *Quarterly Business Process Council* - *Functional Workshops* - *Daily Standups* - *Weekly Sprint Demo, Sprint Retrospective, and Sprint Planning, PI Planning* *All Meetings need to be documented and scheduled.*

PHASE ACTIVITY: REQUIREMENTS GATHERING

This phase focuses on capturing detailed requirements provided by business stakeholders. All requirements should include details from Project Charter and/or Statement of Work (SOW).

NOTE: If Pre-Planning activities occurred prior to the start of the Project Implementation, then the below activities will be to recertify the completeness and accuracy of the artifacts that were produced.

Task	Documents / Steps	More Information
Review and comply with Data Protection Handbook	☐ Data Protection Handbook **(Required)**	**Data Protection Handbook –** *Provides best practices and approved technologies for securing structured and unstructured data (databases, files, emails, SharePoint). Covers encryption, access control, monitoring, vulnerability assessment, backup/recovery, and external sharing. Includes RACI roles, cost considerations, and incident reporting guidance.* **This document should be referenced throughout all phases of the project from Plan to project closure activities.**
Define Project Requirements	☐ Business Requirements Document Template (BRD) **(Required Approval)** ☐ User Stories and Sprint Breakdown *(if using Scrum)*	**Business Requirements Document Template (BRD) –** *Detail the project requirements as laid out in the SOW and/or project charter which highlights the business goals. It also contains sections for functional/non-functional requirements. The Business Lead or Sponsor approves the BRD. The Steering Committee or designee signs off on significant customizations. The document is to contain:* - *Core application description that satisfies requirements* - *Functional design documentation* - *Current state system and business functions* - *Desired changes to current state* - *Visuals or workflow diagrams.* - *Fit/Gap of the functional requirements* - *A matrix of all Key Business Design decisions and approvals* - *A matrix for all Key Data Fields changes* - *Business Process Designs –end-to-end flows of functional processes* - *Current state and future state process flows.* - *Business SOX Requirements Matrix* - *Detailed non-functional requirements (documenting performance targets, scalability requirements, security controls, availability targets (uptime, RTO, RPO), usability standards, accessibility standards (WCAG 2.1 Level AA for customer-facing applications), and maintainability needs).*

Task	Documents / Steps	More Information
		<u>Epic, Feature, User Stories and Sprint Breakdown</u> – *Narrate and/or create use cases to articulate the functionalities. This document should include the functionalities accepted within scope and converted into Epics or a journey of the user and actions are taken within the system. The development team should be responsible for breaking each epic into features and converting each feature into a set of stories for a sprint. A sprint is an iteration of a small set of actions to deliver a functionality. Acceptance Criteria should be obtained from the product owner. These stories should be broken into tasks for easier assignment and tracking.*
Create Data and Mock Conversion Strategy and Execution Plan	☐ Data Conversion Strategy and Plan Template (**Required**)	**<u>Data and Mock Conversion Strategy and Execution Plan</u>** – *The ETS Lead creates this document if the project involves data conversion or migration.* *The plan describes:* - *Data flow from source to target systems* - *Data assessment (source systems, data volume, data quality)* - *Data quality metrics and acceptance criteria* - *Data transformation rules and mapping* - *Data reconciliation approach (source to target validation)* - *Integration with other systems* - *Business validation procedures* *See Data Conversion Strategy and Plan Template for complete structure.* *Mock Conversion plan will identify the approach surrounding the number of conversion cycles, the associated source systems, and master, ancillary, and transactional data reconciliation. Any application replacement or upgrade that involves restructuring a data dictionary requires a data conversion plan.* *Business users define validation procedures to verify accuracy, validity, and completeness of the converted data, then execute the data conversion plan. Create an execution plan that outlines a proposed mock conversion timeline including all source systems, reconciliation plan, and execution window. This plan will be refined continuously from learnings with each Mock Conversion.* *Project Manager should keep in mind data retention for legacy applications and account for this cost. plan for cost of data retention / disposition of the system: refer to* 870- 1 CI Records Management (sharepoint.com) *Document used to track all integrations between systems.* *These documents will be refined throughout the project.*

Task	Documents / Steps	More Information
Create RICEW Object Catalog	☐ RICEW Catalog - SAMPLE	*Include a current state integration diagram* *Identify Edge System impact for integrations and parallel programs (XXPARs)* *Review Key Technical Decisions related to RICEW objects and Middleware* *NOTE: Integrations review will need to include all aspects of Middleware requirements* *These documents will be refined throughout the project.*
Infrastructure Strategy	☐ Infrastructure Example Diagram ☐ Infrastructure Strategy Template	**Infrastructure Strategy** – *The ETS Lead creates the Infrastructure Strategy documenting the technical infrastructure required to support the application.* *The Infrastructure Strategy includes:* - *Server and compute requirements (on-premises or cloud)* - *Database capacity planning* - *Storage requirements* - *Network requirements and bandwidth* - *Containerization approach (if applicable)* - *Backup and recovery approach* - *Monitoring tools and approach* - *Environment planning (DEV, SIT, UAT, Training, Production)* - *Disaster recovery approach (RTO/RPO targets, DR architecture)* - *Disaster recovery testing approach (frequency, scope, success criteria)* - *Cybersecurity testing approach* *See Infrastructure Strategy Template for complete structure.* *Tools assessment is also needed for monitoring, code migration, data replication, defect tracking, and database management. Additional infrastructure strategy will need to include cloud services, middleware, VM etc.* *Review Key Technical Decisions regarding Infrastructure, Middleware and Cloud services.* *These documents will be refined throughout the project.* *A dedicated team of infrastructure SMEs should be assigned to the project.*

Task	Documents / Steps	More Information
Middleware and other Services --- e.g., Cloud Strategies	☐ Middleware Diagram ☐ Integration Architecture Template	**Integration Architecture** – *The ETS Lead with support from the technical team creates the Integration Architecture documenting how the application will integrate with other systems. The architecture includes:* - *API strategy (if applicable): REST/SOAP standards, versioning approach, authentication method (OAuth, API keys), rate limiting requirements, API gateway selection* *For questions or guidance on integration architecture, contact the Integration Services team at dl - IT Integration Services Leads dl-ITIntegrationServicesLeads@coned.com* *Tools assessment is needed for monitoring, code migration, data replication, defect tracking, and database management.*
SOX Controls	☐ SOX Controls **(Required if SOX Application)**	*A matrix outlining all required SOX Controls for User Access, Integration Control, etc.*
Testing Strategy	☐ Testing Strategy Template **(Required)**	**Testing Strategy** – *The ETS Lead creates the Testing Strategy in collaboration with the Business Lead. The strategy defines testing sequence, entry/exit criteria, roles and responsibilities, test data approach, defect severity definitions, and defect management process.* *The strategy addresses these testing phases: Unit Testing, System Testing, System Integration Testing (SIT), End-to-End Testing, Performance Testing, Security Testing, Regression Testing, Parallel Testing (if applicable), and User Acceptance Testing (UAT).* *See Testing Strategy Template for complete structure.*

PHASE MEETINGS

Task	Description
Vendor Onboarding	*Alignment meetings where Vendor is introduced to the working environments and technical aspects of the projects.*

Task	Description
Set up an overall project kick-off	*Set up a meeting with key project members and include the vendor to align and agree on next steps.*
As-is / To-Be Workshops	*series of workshops where the "as-is" and "to-be" states are defined to the lowest level of detail. The detailed requirements are then inputs to the functional and technical designs.*
Deliverables & Business Value Meeting	*Set up a meeting to discuss the required deliverables and business values to meet the business's expectations.*
Project Control Board Meetings	*The Project Manager should set up a project control board at the beginning of your project lifecycle and involve the members from project inception to closure. All board members should have some stake in the project. The Project Manager should align with the control board if decisions are needed beyond the project's scope. Involve SME and advisory members to advise when major decisions are needed.*
Business Sponsor and Project Manager meet to review and approve documentation.	*The purpose of this meeting is to review the key activities and documents and to obtain the Business Sponsor's approval of the Detailed Business Requirements document (BRD), which is necessary to move on to the next phase.*

PHASE ACTIVITY: PLAN ENTRY/EXIT CRITERIA

Entrance	Exit
☐ The Business Sponsor approved the Project Charter (documented approval) ☐ The ETS Lead completed CREATe registration and obtained initial approvals ☐ The Project Manager established ETS Project Repository ☐ The ETS Executive approved the cost estimate ☐ Funding secured and POET obtained ☐ Vendors selected and contracts executed (if applicable)	☐ The Business Sponsor approved functional requirements (documented approval) ☐ The ETS Lead approved technical design (documented approval) ☐ The ETS Lead completed all six CREATe reviews and obtained approvals ☐ Security Architecture Review completed and risks accepted ☐ The Project Manager baselined the project plan ☐ The ETS Lead completed the System Test Plan ☐ The Business Lead completed the OCM Plan ☐ All Plan Phase deliverables complete and approved

PHASE 3: BUILD

PHASE ACTIVITY: DESIGN & DEVELOPMENT

After requirements approval, the development team begins software development activities including user interface design, application configuration, and custom development. Development follows the project management plan and technical design approved in the Plan Phase. The ETS Lead oversees development activities. A substantial portion of the project budget, resources, and time is consumed during this phase. If a change request is submitted during this phase, approval is required before proceeding. Approved changes trigger updates to the management plan and project requirements. The development and delivery of system functionality can be done in an Agile manner where iterations / sprints are completed based on an agreed upon set of functionalities to be delivered per iteration or a Waterfall methodology.

NOTE: Before development begins, the ETS Lead validates that infrastructure environments for the target application, edge systems, and middleware are available, smoke tested, and ready to receive data. Data conversion activities should be stable and ready to move converted data into target environments to support design workshops and unit testing.

Task	Documents / Steps	More Information
Readiness to Build	☐ Readiness to Build Checklist, CREATe **(Required)** ☐ Review 8.13 Secure Coding Guidelines Reference Architecture **(Required)**	**Readiness to Build Checklist** – *Development begins after items on the Readiness to Build Checklist are completed and submitted by the CREATe Requestor or Systems Manager. If Severity 1 items are incomplete, development does not proceed. The ETS Lead is responsible for documenting any exceptions with risk mitigation plans and obtain ETS Executive approval.* *Readiness to Build Checklist is available through CREATe App. Please use the link above to find an exported reference for the checklist* *The checklist verifies:* - *Requirements approved and baselined* - *Technical design approved and baselined* - *All CREATe reviews approved* - *Development environments provisioned and tested* - *Development tools and licenses obtained* - *Source code repository configured* - *Development team access configured* - *Development standards and conventions documented* - *Unit testing approach defined* - *Code review process defined*

Task	Documents / Steps	More Information
		The Transition to Run Checklist (detailed in Test Phase) is begun after the Readiness to Build Checklist is complete. **Secure Coding Guidelines** – *Developers are responsible for reading and following secure coding procedures. See 8.13 Secure Coding Guidelines Reference Architecture for detailed guidance on secure coding practices, GitHub integration, and platform-specific guidance (web, mobile, data security).*
Build Solution Architecture Based on BRD / Technical Specifications	☐ System Design Description (i.e., Technical Design) **(Required)**	**Develop Application Based on Approved Design** – *The development team builds the application based on the approved Technical Design Document and Business Requirements Document (BRD).* *Revise RICEW Catalog, Middleware and Edge integration inventories* *Revise Infrastructure Diagram and Strategy, environments matrix, capacity planning including middleware* *The technical design needs to have signoff by all relevant stakeholders in this step.*
Conduct Unit Testing	☐ Unit Test Plan Template **(Required)**	*Unit test cases are created for functions and methods. Unit testing helps identify and resolve faults introduced by code changes early in development. The purpose of unit testing is to examine each component of the program or application individually to verify that they work as intended.* *Note: Unit testing focuses on individual code components in isolation. Integration testing with middleware and edge systems occurs during System Integration Testing (SIT) in Phase 4: Test.* *The Project Manager allocates adequate time and resources for unit testing.*
Proceed with Data Conversion activities	☐ Data Conversion **(Required)** ☐ Revisit Data Protection Handbook **(Required)**	**Execute Mock Data Conversions** – *The ETS Lead executes mock data conversion cycles to test and refine the data conversion process. Each mock conversion provides learning to improve data quality, transformation rules, and reconciliation procedures. Recommended approach:* - *Minimum 2 mock conversion cycles (3-4 cycles for complex data conversions)* - *First mock: Validate conversion logic and data mapping*

Task	Documents / Steps	More Information
		- *Subsequent mocks: Refine data quality, validate business rules, test performance* - *Final mock: Full production-volume test with complete business validation* *Business users validate converted data for accuracy and completeness after each cycle.* *Any replacement of an application or upgrade of an application that involves a restructuring of a data dictionary requires a data conversion plan. Business users define business validations to be performed to assure accuracy, validity and completeness of the converted data and then execute the data conversion plan validations.* *Revisit Data and Mock Conversion Strategy documents and reference the data protection handbook.*
Comply with *ETS* guidance for application security	☐ Secure Coding Procedure **(Required)** ☐ CREATe - Checklists & Forms (CREATe)	*Facilitates information for developers and build teams to adhere to secure coding procedure and to recommended guidelines.* *The design is expected to adhere to published ETS guidance regarding application security. The ETS Project Manager and/or Project Lead works closely with the information security team to obtain checklist approval and address all relevant security considerations. This collaborative approach ensures that any potential security gaps are identified, assessed, and appropriately mitigated or resolved.* *Application Security Checklist is available through CREATe SharePoint Portal linked above and only required for CREATe requests that pertain to application builds.*
Execute Mock Conversions	☐ Mock Conversion	**Mock Conversions –** *The ETS Lead executes multiple mock conversion cycles to test and refine the data conversion process. Each cycle copies production data to the UAT environment in accordance with company data protection guidelines. Business users validate converted data for accuracy and completeness after each cycle. The ETS Lead approves each mock conversion plan and execution (email approval).*

Task	Documents / Steps	More Information
Conference Room Pilot	☐ Conference Room Pilot Log Template **(Required)**	*Conference Room Pilot (CRP) – CRPs validate that the configured or developed application meets business requirements before formal testing begins. CRPs allow business users to see working functionality and provide feedback early when changes are easier and less expensive to implement.* *Conduct CRPs at key milestones:* - *CRP 1: After 30-40% of development complete (validate core functionality)* - *CRP 2: After 70-80% of development complete (validate integrated workflows)* - *CRP 3: After 95% of complete development (final validation before system testing)* *See CRP Feedback Log Template to capture feedback from each session. Categorize feedback as:* - *Critical: Must fix before UAT* - *High: Should fix before UAT* - *Medium: Can defer to UAT or post-go-live* - *Low: Future enhancements.* *The Business Lead facilitates CRP sessions with business SMEs and power users. The development team demonstrates functionality and addresses feedback.*
Review the need to submit a Scope Change Request	☐ Scope Change Request Form Template **(Required)**	*Log scope changes are required to determine priority and next steps**.** The Project Manager should stay up to date with the Change control Board as planned in the Change Control Plan documentation. The Change Control Board manages scope changes considering project schedule and budget impact.*
Conduct RICEW Object Catalog Comparison	☐ RICEW Catalog - SAMPLE	*Once the Design Phase of the Systems Development Lifecycle (Waterfall or Agile) is complete, compare the new or revised RICEW Object Catalog to the original from the Business Case or Statement of Work to assess any changes in scope or effort required.*

Task	Description
Technical Review	*Assigned project members may engage with team members outside the project to review both the Requirements Document and the System Design Document for feedback. This process should also confirm adherence to ETS Procedures where relevant. Participation from the ETS architect or a representative from EA is recommended as part of the review team.* *Approval is required by ETS Lead.*
Code Review	**Code Review –** *Structured sessions where developers present their code to peers and the ETS Lead for feedback and improvement. The objective is to validate that code is consistent, readable, secure, and meets design expectations. Code scanning and analysis tools should be used to identify security vulnerabilities, code quality issues, and technical debt. Developers are responsible for reading and following the secure coding procedures. For secure coding guidance, see: 8.13 Secure Coding Guidelines Reference Architecture. The meeting's objective is to validate code consistency, readable, secure, and meets design expectations. Someone from EA should be part of the review team.* *Code scanning and analysis tools should be used in this step if available.* Developers and build teams should read secure coding procedures and adhere to recommended guidelines.
Testing Meeting	*Meeting where programmers and testers collaborate to plan, execute, and evaluate the testing of the code. The meeting's objective is to verify that the code is functional, reliable, and meets business requirements.*
Status Update	*Meeting where programmers report their progress, challenges, and issues to the Project Manager and other stakeholders involved in this phase. The meeting objective is to monitor the project schedule, budget, and quality. Meetings should occur at agreed-upon intervals.*
***SCRUM Ceremonies* – Meetings to address and plan an iteration and drive it to completion.**	
Sprint Planning	*After determining the scope of the sprint, Project Manager/ETS Lead estimates the amount of work required for each story in the sprint, such as time/effort needed. This also includes designing an approach to proceed.*

Task	Description
Daily Stand-up Meetings	*The development team meets to discuss the sprint progress for 15 minutes. The meeting is designed as a high-level discussion meant to inform others of the work completed, work to be done, and expected challenges.*
Sprint Review	*After completing the development work needed for the sprint, the changes are demonstrated to the user. This is to verify that the implementation matches the user's desired results. The user can provide feedback on the work presented.*
Retrospective	*The development team reviews and acts on the feedback received. This is also the opportunity for the development team to discuss lessons learned and other development process improvements for future sprints.*

PHASE ACTIVITY: BUILD ENTRY/EXIT CRITERIA

Entrance	Exit
☐ Business Sponsor approved functional requirements (documented approval) ☐ ETS Executive approved technical design (documented approval) ☐ All six CREATe reviews completed and approved ☐ Project plan baselined ☐ Development environments ready and smoke tested ☐ Readiness to Build Checklist complete and approved ☐ Development team onboarded and trained	☐ All development complete per approved requirements and design ☐ All unit testing complete with no critical defects and meets defined threshold ☐ Code review complete and approved ☐ All Conference Room Pilots (CRPs) complete with feedback addressed ☐ System Test Plan finalized and approved ☐ Test environments ready for System Testing ☐ Test data loaded and validated in test environments ☐ All build phase deliverables complete and approved

PHASE 4: TEST

PHASE ACTIVITY: SYSTEM TESTING

Test Phase focuses on conducting a thorough testing to verify the application meets requirements and is ready for production. The project team conducts multiple testing phases in sequence: System Testing, System Integration Testing (SIT), Performance Testing, Security Testing, and User Acceptance Testing (UAT). The project team conducts testing following the approved Testing Strategy and System Test Plan created in the Plan Phase.

Task	Documents / Steps	More Information
Define System Test cases and Data Conversion Validations	☐ Revisit Data Protection Handbook **(Required)** ☐ Review PB.SEC.01 - Application Security Testing Guideline **(Required)** ☐ Data Conversion Plan validation ☐ System Testing Plan Template **(Required)** ☐ Requirements Traceability Matrix Template **(Required)**	**Application Security Testing Guideline** – *This guideline defines how to conduct Static (SAST) and Dynamic (DAST) security testing, including vendor-hosted app scans and open-source code reviews. It also outlines compliance requirements before production release.* **Data Conversion Plan Validation** – *Any application replacement or upgrade that involves data dictionary restructuring requires a data conversion plan. Business users define business validations to be performed to validate accuracy, validity and completeness of the converted / migrated data and then execute the data conversion plan validations.* **System Test Plan Template** – This document outlines the procedures to be followed during system testing. The test plan specifies the types of tests to be conducted, the required environment, and delineates team roles and responsibilities. The Testing Team is responsible for developing the system test plan and implementing it during the System Testing phase. The composition of the Testing Team is determined during the planning stage. If a Testing Center of Excellence is in place, ETS should be consulted to conduct a thorough review and alignment of the overall testing plan. *At this point of the project, the following test levels should be achieved:* - *System Integration Testing (SIT)* - *End to End Test* - *Regression Testing* - *Parallel Testing (if applicable)* - *Dress Rehearsals* - *Operational Readiness Testing* - *Performance Test / Stress Test* - *Any other tests applicable to the application.* - *System Acceptance Testing*

Task	Documents / Steps	More Information
		Requirements Traceability Matrix Template – *The RTM is created to log all your requirements and trace back to the different test cases, business processes, change impacts, and defects.*

PHASE ACTIVITY: TESTING STRATEGY AND EXECUTION

The focus of this phase activity is testing the functionality as it applies to the end user. Any defects identified in the software are reported and prioritized based on business needs for correction and re-testing. The Project Manager completes all documents and obtains the Business Sponsor's Approval.

Task	Documents / Steps	More Information
Define Test Strategy and Data Conversion Plan	☐ Revisit Data Protection Handbook (**Required**) ☐ Stage Data ☐ User Acceptance Test Plan Template (**Required**) ☐ Defects List Template (**Required**) ☐ Defects Management Plan (**Required**) ☐ Test Cases Template (**Required**) ☐Testing Evidence (**Required**) ☐ Credentials Template	**Stage Data** – *The ETS Lead with support from the technical team may stage test data to support users in testing the system and validating workflows. This activity is optional.* **Test Strategy and Plan Template** – *Describe the background, strategy, detailed procedure to be followed during the test, and the expected results. The test plan should be simple, but clearly define what is to be done, how it will be done, who will do it, and when it will be done. Responsibility for development of the user testing plan falls to the user of the system, usually the Business Lead and their team. This same business lead has the responsibility of final sign off.* **Defects List Template** – *Testers log all failed test cases in the defect tracking tool. See Defect Management Plan for complete defect workflow and severity definitions.* **Defect Management Plan –** *Defects identified during any testing phase (System Testing, SIT, Performance Testing, Security Testing, UAT) are logged and managed using a process that includes:* - *Defect Logging* - *Defect Triage* - *Defect Resolution* - *Defect Retesting* - *Defect Reporting* - *Defect Approval Criteria for Production* **UAT Test Assignments** – *Document should be prepared before scheduled UAT session. Should include:* - *Tester names and contact information*

Task	Documents / Steps	More Information
		- *Business roles represented by each tester* - *Test scenarios assigned to each tester* - *Test environment access credentials (if needed)* **Test Cases Template** – *Document is to describe the steps needed to be followed by user to validate the functionalities in scope.* **Testing Evidence** – *Includes the list of Business Requirements tested and screenshots showing the working results.*
User and Training Manual Creation	☐ User Manual Template (**Required**) ☐ Job Aid	**Create User Training Materials** – *The Business Lead creates user education materials including user manuals, job aids, quick reference guides, and training presentations. Training materials should be reviewed and approved before training delivery.* **User Manual Template** – *Step-by-step process of system workflow and functionalities available for the user. The Business Lead creates the document after UAT completion to verify end-user understanding of system functionality. A business analyst then checks the document to flag any misunderstandings.* **Job Aid** – Guides to operate and work on a specific function or role.
Confirm Go-live Readiness	☐ User Acceptance Exit Criteria Template (**Required Approval**)	**User acceptance Exit Criteria Template** – The Business Lead or Sponsor approves release of the system to the production environment. *At this step, the deployment plan initiated in the plan phase is expected to be finalized.*

PHASE MEETINGS

Task	Description
Post System Testing Go/No-Go Meeting	*Set-up a meeting with responsible stakeholder group to confirm readiness to begin User Acceptance Testing (UAT).* *There needs to be a Business / ETS Readiness Matrix that each functional and technical stakeholder provides concurrence for GO-NO-GO decision with predefined categories for acceptance*

Task	Description
Train the Trainer Workshops	Meeting hosted by a system expert to demonstrate functionalities to UAT tester to test during the UAT. This session is conducted with a small group of users / Power Users.
UAT Sessions	Sessions scheduled for a specific duration to test in-scope system functionalities and address end user feedback.
Conduct a Production Go-no-Go Meeting	A written approval to go-live should be gained from the Business Sponsor. Project Manager may use the User Acceptance Exit Criteria. The meeting is to be held with the stakeholder group responsible to confirm readiness to go-live and release system into the production environment.

PHASE ACTIVITY: TEST ENTRY/EXIT CRITERIA

Entrance	Exit
☐ Build Phase exit criteria met ☐ All development complete and unit testing passed ☐ Test environments ready and validated ☐ System Test Plan approved ☐ Test data loaded and validated ☐ Test team trained and has access to testing environments	☐ All planned testing complete (System, SIT, Performance, Security, UAT) ☐ Severity 1 and 2 defects have been fixed and tested, or an approved workaround has been documented ☐ Business Sponsor approved UAT results (documented approval) ☐ User training complete with attendance documented ☐ User documentation and job aids finalized ☐ Production Readiness Review complete ☐ Production go/no-go decision approved by Business Sponsor and ETS Executive

Note: Detailed entry/exit criteria for specific test types (SIT, Parallel Testing, UAT, Performance Testing) are documented in Attachment 6: Test Entry/Exit Criteria Reference.

System Integration Testing (SIT): System Integration happens upon successful completion of the Build phase and unit testing.

Entrance	Exit
☐ There are no scope change requests open or in progress which impact the SIT case execution, or there is a regression test plan in place ☐ System Integration Test plan/strategy has been completed, reviewed, and approved ☐ Test cases for SIT iteration have been identified and approved ☐ SIT environments are available and code/configuration for SIT iteration has been deployed ☐ Test data representing realistic user scenarios has been loaded in UAT environment per test data requirements ☐ Testers have been identified, trained, and provided access to testing environments ☐ Smoke testing completed for interfaces defined in scope for SIT iteration ☐ All severity 1 and 2 defects identified in smoke testing are fixed and deployed in SIT environments or a work around has been approved and communicated ☐ Test cases and results from prior test phase have been documented ☐ Requirements traceability document is ready for testing	☐ Planned test cases for SIT have been executed per the test plan ☐ Requirements traceability document has been completed ☐ All test results have been reviewed and captured ☐ All severity 1 and 2 defects have been fixed and tested, or an approved work around has been documented ☐ All remaining open/failed defects are reviewed and there is a plan in place to address them ☐ A formal Go/No-Go meeting is held

Parallel Testing: Validate that the new system produces results consistent with the current production system by running both systems simultaneously with the same data inputs.

Entrance	Exit
☐ Test cases for Parallel Testing iteration have been identified and approved by the Business Lead ☐ System Integration Testing (SIT) has been completed successfully ☐ All severity 1 and 2 defects identified in unit testing, system testing, and SIT are fixed and deployed to Parallel Testing environment, or approved workarounds have been documented and communicated ☐ Smoke testing for full data conversion is complete and accepted. Data migration defects are understood and quantified for business impact ☐ Production configuration data (prices, rates, rules, reference data) has been updated in Parallel Testing environment ☐ Test data files are prepared and validated ☐ Interfacing systems are integrated and refreshed with appropriate test data ☐ Parallel Testing dry run is complete. Tools required for parallel testing are ready and tested. Comparison functionality is working as expected	☐ 100% of planned parallel test cycles have been executed successfully ☐ All Parallel Testing deliverables are completed, accepted by the Business Lead, and published ☐ Results from the new system match production system results, or discrepancies are explained, documented, and approved by the Business Sponsor ☐ All severity 1 and 2 defects identified during Parallel Testing have been fixed and retested, or approved workarounds have been documented ☐ All remaining open defects are resolved, or the Business Sponsor has approved them as acceptable open defects with documented business impact and mitigation plans ☐ The Business Lead has documented approval that Parallel Testing results demonstrate the new system is ready to proceed to User Acceptance Testing

User Acceptance Testing (UAT): Testing the functionality as it applies to the end user.

Entrance	Exit
☐ System Integration Tests have been completed successfully ☐ There are no scope change requests open or in progress which impact the UAT case execution, or there is a regression test plan in place ☐ User Acceptance Test plan/strategy has been completed, reviewed, and approved ☐ Test cases for UAT iteration have been identified and approved ☐ UAT environment is available and code/configuration for UAT iteration has been deployed ☐ Sufficient test data representing realistic user scenarios has been identified and loaded in UAT environment ☐ Testers have been identified, trained, given credentials to access testing environment, and provided a way to report defects ☐ Inbound and outbound interface (both real time and batch process) are operating and communicating ☐ Smoke testing completed for interfaces defined in scope for UAT iteration ☐ Open/failed defects and defects with workarounds are provided to testers ahead of beginning the UAT session ☐ Test cases and results from prior test phase have been documented	☐ 100% of test cases planned for UAT have been executed ☐ All test results have been reviewed and captured ☐ All severity 1 and 2 defects have been fixed and tested, or an approved work around has been documented ☐ All remaining open/failed defects have been identified as future enhancements, and there is a plan to address them ☐ A formal Go/No-Go meeting is held ☐ Preparations for a Dress Rehearsal have been made

Performance Testing: Testing to measure non-functional aspects of an application under a specific workload.

Entrance	Exit
☐ Performance test plan/strategy has been completed, reviewed, and approved ☐ Test scripts and scenario designs have been completed ☐ Dedicated production like performance test environment is made available throughout the testing timelines ☐ End-to-end infrastructure connectivity is established between architectural components ☐ Adequate stage data has been identified and is available in performance test environments ☐ Performance testing and monitoring tools are configured as required	☐ 100% of planned performance scenarios and runs have been executed ☐ SLA's have been met ☐ Performance bottlenecks have been identified, raised, and tracked using the defect management tool ☐ All the test results have been reviewed and captured ☐ Performance testing results or summary reports are reviewed and signed off ☐ No open defects are observed during test ☐ All System Testing and SIT are complete with all Severity 1 and 2 defects resolved. Application is functionally stable with no known critical defects

PHASE 5: DEPLOY

The Deploy Phase focuses on deploying the application to production, providing Hypercare support, and transitioning to ongoing operations. The ETS Lead executes production deployment following the approved Deployment Plan. The project team provides intensive Hypercare support for 4-12 weeks after go-live. The ETS Lead transitions the application to the operations support team.

PHASE ACTIVITY: PRE-DEPLOYMENT

Before releasing the system to production, complete the following activities to verify documentation is available and confirm the system is ready for release.

Task	Documents / Steps	More Information
Prepare for Production Migration	☐ Revisit Data Protection Handbook ☐ Revisit PB.SEC.01 - Application Security Testing Guideline ☐ Transition to Run Checklist, CREATe **(Required)** *Transition to Run Checklist is available through CREATe App. Please use the link above to find an exported reference for the checklist.*	**Transition to Run Checklist** – *The ETS Lead completes the Transition to Run Checklist before production deployment. Complete and submit all checklist items through the CREATe application before production deployment. The checklist verifies production readiness including infrastructure, security, monitoring, support processes, and documentation.* **Data Conversion Plan Execution** – *Complete data conversion and load data to production database.* **Deployment Plan Template –** The document's content should be collected throughout the project and finalized before production deployment. The purpose of the Deployment Plan Template is to provide details in the event of issues arising upon proceeding to production deployments. *It includes the rollback and backout plan.* **Release Notes Template –** *The document's content should be collected throughout the project and finalized before production deployment. Before deployment, this document should be released to stakeholders for approval on procedures. This is to be released after the completion of production to everyone involved.* **Managed Service Provider** – *The content of the folder includes references to provide application support that meets the needs of the business and supports the reliability and performance of the applications. This involves smooth handover from development to support teams, continuous monitoring and maintenance of operational processes, and effective governance of application health and stability.*

Task	Documents / Steps	More Information
	☐ Data Conversion Plan ☐ Deployment Plan Template ☐ Release Notes Template ☐ Managed Service Provider(s) References	

PHASE ACTIVITY: POST DEPLOYMENT

The post go-live period is a part of the project and is to be managed by the project team assigned to develop and implement the application/system. This includes vendors, staff augmentees, and contractors. This phase is also an opportunity to accurately confirm the level of support the new application/system will need and responsible members needed.

- If application support is going to remain internal, the *ETS* run team, business, and business support will be needed.
- If the application/system support is going to be outsourced contact the Vendor Management Office
- Identify the Business Support team
- After go-live, systems transition to the O&M support model.
- Future phase or day two (2) work are expected to be planned and is capitalized as stand-alone projects (i.e., version 2.0')

Task	Documents / Steps	More Information
Deployment Verification	☐ Review ISP-401 Vulnerability Management Program ☐ Prod User Smoke Testing ☐ Basic Regression Test Verification Template **(if needed)**	**Vulnerability Management Program** –*This policy governs how vulnerabilities are identified, triaged, remediated, and tracked post-deployment. It includes scanning schedules, exception handling, and reporting protocols for live systems.* **Production Verification Testing –** *Immediately after production deployment, designated business users and technical team members execute production verification test cases to confirm deployment success and system functionality. Production verification testing includes smoke testing of critical functionality, verification of integrations, and confirmation that users can access the system. The Business Lead and ETS Lead assign team members to execute specific verification tests.* **Basic Regression Test Verification Template** – *Listing the team member responsible for performing the test and the high–level functionalities and steps to be followed to verify the production environment after the production deployment. If defects are found and the deployment is for system fixes, regression testing is recommended.*
Finalize and Release Post-Deployment Documentation	☐ Release Notes Template	**Release Notes Template –** *Release Notes content should be gathered throughout the project, then reviewed and finalized before production deployment. Prior to deployment, share this document with stakeholders to obtain approval on all procedures. Once production is complete, distribute the finalized version to everyone involved.* *The ETS Lead finalizes all post-deployment documentation including as-built documentation, updated technical design, production configuration, and lessons learned. The Project Manager releases the Release Notes to all stakeholders. Release Notes summarize what was deployed, known issues, and next steps.*

PHASE ACTIVITY: HYPERCARE

Hypercare Support – Enhanced support commences immediately following production deployment. The project team provides enhanced support to resolve issues, optimize performance, and supports user adoption. Hypercare typically lasts 4-12 weeks depending on project complexity and risk. As a guideline, plan for one month of Hypercare for every twelve months of development. The ETS Lead defines Hypercare duration in the Deployment Plan.

As a guideline, plan for 1 month of Hypercare and 3 months of stabilization for every 12 months of development activity. During this stage, the vendor or development team assists users with system adoption and issue resolution. Once the system meets Hypercare exit criteria, it transitions to the long-term support team. Depending on project complexity, prepare appropriate documentation and resources before Hypercare begins to support application sustainment. Prepare the following documentation to support application sustainment:

- Detailed transition plan
- Knowledge transfer documents
- Functional and technical documents
- Technology stack information including interfaces (inbound/outbound)
- Application and infrastructure architecture details
- Disaster Recovery Plan
- Non-functional requirements (performance, browser support)
- Source code

Hypercare exit criteria should be agreed upon before go-live. A common practice is to resolve all Priority 1 (P1) and Priority 2 (P2) items before exit. Priority 3 (P3) items and future enhancements are documented for the support team.

After Hypercare, the project typically enters a warranty period (typically 90 days) where the System Integrator (SI) provides defect support under contract terms. The warranty period follows Hypercare (does not overlap). During warranty, the SI resolves defects while the long-term support team continues operational support. The ETS Lead manages warranty period activities and tracks defect resolution. After the warranty period, the application transitions fully to the long-term support model.

STABILIZATION

This phase follows Hypercare and marks when the application or system reaches stability. Major bugs and enhancements are addressed during this time.

- Application/system ticket information for 3 – 6 months (if available)
- Defect/ticket backlog from development, with plan to complete before hand-off
- Estimated annual support hours (or actuals if available)
- Support hours requirement / Medal category (support tier classification)
- Application non-ticketed activities including monitoring effort and monitoring tool
- Actual user base and estimation of growth
- License / subscription Requirements

TRANSITION FROM BUILD TO RUN OPERATIONS

Option 1: Bring in the support team to the project to be involved in the pre-deployment phase.

Option 2: Bring in the support team to the project after hyper-care period. Verify that the documents mentioned above are provided to the team.

For applications transitioning to a Managed Service Provider (MSP):

- Hypercare: 4-12 weeks (project team support)
- Warranty Period: 90 days (SI defect support)
- MSP Knowledge Transfer: 2-3 months (overlapping with warranty)
  MSP Transition: 1 month (MSP assumes full support)
- Total timeline from go-live to MSP full support: 6-9 months

The MSP should be engaged during Hypercare to observe support activities, understand the application, and prepare for transition.

In addition, the following is also required:

- Tickets Data (Hypercare and 2-3 months of data from Stabilization).
- 2 months for MSP In-take.
- 1 month for onboarding + transition.
- Functional documentation
- Non-functional requirements (performance, browser support etc.,)
- Technology stack including interfaces (inbound / outbound)
- App/Infra architecture details
- Current annual support hours
- Application non-ticketed activities including monitoring effort and monitoring tool.
- Monitoring tool and parameters monitored
- Support hours requirement / Medal category
- Current user base
- Current Defect/ticket backlog from development and plan to complete before hand-off.
- Disaster Recovery plan
- License / subscription Requirements
- Vendor Applications –
  - Identify the level of support performed.
  - Identify the level of support expected from long-term support team.
  - Identify the underlying technology of the product.
  - Identify agreement of support coverage by application vendor (if applicable).

Task	**Documents / Steps**	**More Information**
Transition to support	☐ Revisit ISP-401 Vulnerability Management Program ☐ Knowledge Transfer Document Template ☐ Backlog Template **(Required)**	**Vulnerability Management Program** –*This policy governs how vulnerabilities are identified, triaged, remediated, and tracked post-deployment. It includes scanning schedules, exception handling, and reporting protocols for live systems.* **Knowledge Transfer** – *The ETS Lead conducts knowledge transfer to the operations support team. Knowledge transfer includes technical documentation, operational procedures, monitoring procedures, troubleshooting guides, architecture diagrams, integration documentation, and support contacts. The ETS Lead trains the support team on application functionality, common issues, and escalation procedures.* *Knowledge transfer should be documented using a Knowledge Transfer Completion Checklist confirming all required documentation has been delivered, all training has been completed, and the operations team confirms they are ready to support the application independently.* *If the Help Desk supports the application, provide a demonstration and address their questions about system functionality and common issues. Documents should include frequently asked questions, issues and resolutions, and Disaster Recovery Plan.*

Task	Documents / Steps	More Information
		Backlog Template – *Contains issues that carried over from UAT and were not resolved before deployment. The list can also include issues found post-deployment.*

PHASE ACTIVITY: PROJECT CLOSURE

The Project Closure phase is where Project Manager(s) focus on ensuring that all project documentation is placed in its appropriate folder and that PI 360 contains accurate information reflecting the project's accurate status. The transition support team should include:

- Project management team
- Developers and SMEs who can provide knowledge transfer
- ETS System Manager to support the product/application after go-live (run team)
- Outsourced team lead and support team

Task	Documents / Steps	More Information
Retrospective and Document Lessons Learned	☐ Post Project Survey Template ☐ Project Lessons Learned Template	**Post-Implementation Review (PIR) –** *The Project Manager conducts the PIR 60-90 days after go-live.* *The PIR evaluates:* - *Project outcomes against original objectives* - *Schedule performance (actual vs. planned)* - *Budget performance (actual vs. budget)* - *Benefits realization (actual vs. projected)* - *Lessons learned (what went well, what could improve)* - *Recommendations for future projects* - *Outstanding issues and transition to operations* *The Project Manager circulates the Post Project Survey to team members before the PIR meeting to gather feedback. The PIR report is presented to the Business Sponsor and ETS Executive and archived in the project repository.* *If business benefits are not being realized, the Business Lead develops a corrective action plan.*

Task	Documents / Steps	More Information
		Project Lessons Learned Template – *Analyze the things that went well and the things that did not go so well. The lessons learned from the project are documented so the company can benefit from the experience. Evaluate the adherence to the defined project process, and/or compare project's planned vs actual output, and receive feedback and action items to be provided to the applicable people.*
Project Closure	☐ Legacy Application Retirement Plan Template ☐ Project Closure Guide ☐ Register Project Points of contact	**Legacy Application Retirement Plan Template** – *The Business Lead and ETS Lead finalize and execute the legacy application retirement plan if the project replaces an existing system. This plan addresses data retention requirements, system decommissioning, and compliance with CI-870-1 Records Management. The plan is finalized in the Deploy Phase but planning begins in Phase 2 to identify data retention costs and timeline impacts.* **Project Closure Guide** – *Used to enable PMs to close projects in PI 360, hand off to run team, and update project statuses in ETS Project Library. PMs can also off-board vendors as needed.* **Archive Project Documentation –** *The Project Manager organizes all project documentation in the ETS Project Library. Archive final approved versions of all deliverables. Remove draft versions and working documents. Verify that documentation is organized by phase for future reference.* *The Project Manager validates that all project documentation is organized by SDLC phase and includes:* - *All approved deliverables (requirements, designs, plans, test results)* - *All approval documentation (emails, meeting minutes, signatures)* - *All project logs (risks, issues, decisions, change requests)* - *All project status reports* - *Lessons learned and PIR report* - *Final as-built documentation* *The Project Manager removes draft versions and working documents. Only final approved versions are archived. The assets and their properties shall be registered via ServiceNow.*

PHASE MEETINGS

Task	Description
Business Sponsor and Project Manager meet to review and approve documentation	*The Project Manager will meet with the Business Sponsor to get approval to move the system into production.*
Rollback Meeting (if needed)	*After Production deployment, conduct a regression test before handing off to end user if any issues found, prepare to meet with development team to discuss a potential rollback to original state to avoid any delays / interruptions of business user's work time.* *If no issues are found, hand off the system to a super user to conduct a sanity check of the production environment. If any issues are found, plan a meeting to discuss findings and figure out if a rollback will be needed.*
Lessons Learned	*Prior to the meeting, share the Post Project Survey document with team members to gather insights on team members / stakeholders' experience working on the project. Once all the details are provided, set up a meeting to discuss common feedback and trends. Celebrate success and points of improvements found.*
Knowledge Transfer Meeting	*Set up a meeting to verify readiness of run team to take on the system and fully support users.*

PHASE ACTIVITY: DEPLOY ENTRY/EXIT CRITERIA

Entrance	Exit
☐ Test Phase exit criteria met	☐ Application successfully deployed to production
☐ Business Sponsor approved UAT results	☐ Production verification testing complete and passed
☐ Production Readiness Review complete	☐ Hypercare complete with exit criteria met
☐ Deployment Plan approved	☐ Application transitioned to operations support team
☐ Rollback plan tested and approved	☐ Post-Implementation Review (PIR) complete
☐ Production environment ready and validated	☐ Lessons learned documented
☐ Production data loaded and validated	☐ All project documentation archived in ETS Project Repository
☐ Support team trained and ready	☐ Legacy system retired (if applicable)

SECTION 5. SDLC GUIDE DOCUMENT CHANGE MANAGEMENT

This document will be an evolving process to provide an update of the best practices to teams involved in Software Development Projects. There will be appointed members that form a committee that will meet yearly to assess the usage and provide feedback on improvement as it applies to projects and real-world scenarios.

Version History

Version	Change Made	Author	Date
1.0	SDLC Document released	Nadeen Elakkad	02/01/2023
1.1	RACI Added	Nadeen Elakkad	02/09/2023
2.0	General updates: Update to mentions of financial estimator. Update to CREATe Links. Emphasized required documents in each phase plus provided a resource pocket guide. Added a new section to emphasize the Test Entry/Exit Requirements. Added templates / information for outsourced projects.	Nadeen Elakkad	01/02/2024
3.0	Update from Jeannine regarding phase 0 Added link to phase 0 deliverable document. General updates from Director's suggestions: Update to RACI; envision, plan, deploy Update to design phase, Requirements Gathering. Update to testing phase. General updates from Rob C. suggestions: Parallel Project definition	Glenn Hofmann	08/01/2024

Version	Change Made	Author	Date
	RACI; all activities have an 'R' Update to plan phase. Verified that all links are working.		
4.0	Updated multiple sections based on major projects lessons learned and recommendations including the new and updated cost estimation tool	Madhu Reddy	12/31/2024
5.0	**- Value Realization Management (VRM):** Activities for consideration of VRM for projects exceeding $50M in total capital costs. **- Data Security:** Adding Data Protection Handbook and various activities around data security. - Adding references for **Enterprise Application Security and Vulnerability Management:** PB.SEC.01 - Application Security Testing, Secure Coding Guidelines Reference Architecture, ISP-401 Vulnerability Management Program. - Integrating **Phase 0** Deliverables, Activities, and Recommendations. - Updating Link for **Cost Estimating:** Replacing excel estimator with the newly released cost estimating application. - AI: Adding link to **AI Guidelines** as a consideration when applicable. - Adding details for **internal QA process flagging** required documents and requiring the use of a centralized repository. **- Document Usability and Readability**: Addressing feedback about broken links / page spacing. **- Project Status Report (PSR):** To be generated monthly. **- ETS Rebranding**.	ETS PMO	12/26/2025

Approvers

Name	Version #	Position	Date
Jenny Brito	1.0	Director	01/31/2023
William Kearns	2.0	Director	12/12/2023
William Kearns	3.0	Director	08/01/2024
Madhu Reddy	4.0	Director	12/31/2024
Steven Maniscalco	5.0	Department Manager	12/26/2025

1.0 PURPOSE – To establish the process to be followed to register the technical review of an information technology (IT) project as required by Consolidated Edison, Inc. Corporate Instruction (CEI CI) 215 "Acquisition, Development and Deployment of Information Technology". This technical review procedure is applicable to activities covered in the Corporate Request for Evaluation and Approval of Technology (CREATe) Application under CEI CI-215.

2.0 APPLICATION –

2.1 This procedure applies to all organizations of Consolidated Edison Company of New York, Inc. (CECONY), Orange and Rockland Utilities, Inc. (O&R), and Con Edison Transmission, Inc. (CET) requesting a technology project is required by Consolidated Edison, Inc. Corporate Instruction (CEI CI) 215. All organizations are subject to compliance with this Instruction regardless of whether the Information Technology (IT) organization actively performs the project management and/or software development role for a given project. The terms Corporate or Company, when used in this Instruction, refer to CECONY, O&R, and CET unless otherwise stated.

3.0 INTRODUCTION – The Corporate Request for Evaluation & Approval of Technology (CREATe) is a process designed to provide a centralized system for customers to request technical reviews, evaluations, and approvals of IT designs, architectures, and technologies required to implement a project or solution. The process is facilitated via the CREATe Application, which promotes cross-functional team reviews while keeping stakeholders informed on progress. For software-related requests, CREATe is a sub-process requirement of the overarching Software Development Lifecycle (SDLC) Guide.

Adherence to the CREATe process is needed to address the increasing reliance on information technology, growing interdependencies of applications, data, and cybersecurity threats. A single vulnerability in our Information Technology (IT) infrastructure can lead to widespread operational outages across our entire company.

4.0 DEFINITIONS –

4.1 Build – third (3rd) stage of CREATe; collects outputs and approvals from the Review stage using the Readiness to Build Checklist to guide the production of documented details and timelines for building a system.

4.2 Build Team – IT group(s) who help with the development and/or building of a request and can include members from IT, the business, and/or vendors.

4.3 Business Lead – a person representing the business who bears responsibility for the successful delivery of project objectives.

4.4 Business Relationship Manager (BRM) – an IT manager who is responsible for developing and maintaining effective relationships between IT and the business units (advocating for business needs within IT); assigned to a CREATe request to serve as

the liaison between IT and the business Requestor upon its creation.

4.5 **Corporate Request for Evaluation and Approval of Technology (CREATe) –** the process described in this procedure for requesting, vetting, and approving projects.

4.6 **Enterprise Architecture (EA) Architect –** a person who will review and approve the project on behalf of the Enterprise Architecture group. Enterprise Architects provides standards, guidance, and governance for analyzing, designing, planning, and implementing required business & technical capabilities to successfully execute business strategies.

4.7 **Enterprise Program (EP) –** a collection of sub-requests managed as a group over an extended period to achieve efficiencies of scale for the business (i.e., CORE, GIS, REV); EPs are funded at the Program Level (through the Rate Case).

4.8 **Hardware Pilot –** the roll out of a new physical product (hardware, sensor, IoT device, etc.) in real-world conditions to a small area of an organization to evaluate its viability.

4.9 **In-Place Upgrades** – refers to the replacement of an operating system (OS) or application without first removing the older version and without saving any data.

4.10 **Information Security (Cyber) Analyst –** a person who will review and approve the request on behalf of the Cyber Security group.

4.11 **Information Technology** – information and communication systems, applications, databases, platforms, and infrastructure, including cloud technologies and Operational Technology (OT) systems and devices.

4.12 **Intake** – first (1st) stage of CREATe; requestor submits a new request and uploads required documents (including forms) for a BRM and Systems Manager to review and accept into their portfolio(s).

4.13 **IT Lead –** a person representing the IT organization who bears responsibility for the successful delivery of project objectives. This person is also specifically responsible for adherence to IT procedures and processes relevant to the project; this could be a Systems Manager, Business Relationship Manager, Enterprise Architect, Cyber (InfoSec) Analyst, or another IT employee.

4.14 **Project –** a time limited initiative that involves the development, acquisition, and/or deployment of information technology with a plan of action to produce a deliverable and/or achieve a particular goal (i.e. unique service, asset, or result); a project can be a standalone initiative or part of an Enterprise Program (EP).

4.15 **Project Manager –** an individual leading project management activity on behalf of the project; this could be the Requestor, Systems Manager, IT Lead, Business Lead, or a shared ownership model.

4.16 **Project Sponsor –** the person who sponsors the project on behalf of their organization; the sponsor establishes the vision and scope of the project and supports overall project objectives; they also ensure budget and resource availability.

4.17 **Proof of Concept (PoC)** – an experiment intended to demonstrate that a design concept or business proposal is feasible for real-world deployment.

4.18 **Other Involved Personnel** – those added to a request as read-only participants so they can view/track the request's progress and details.

4.19 **Readiness to Build Checklist** – the in-app checklist presented at the beginning of the Build stage (after receiving approval in Review); connects project team with IT groups to ensure requests do not deviate from established reference architecture, blueprints, and design standards while beginning development work.

4.20 **Review** – second (2nd) stage of CREATe; EA and Cyber perform a technical review of a request from their areas of expertise and offer a decision to proceed (Approved, Rejected, or More Info Needed).

4.21 **Request for Proposal (RFP)** – the evaluation of a vendor's product or contractor's ability to undertake a project initiated through the distribution of an RFP (business document that announces a project and solicits bids from qualified contractors to complete it)

4.22 **Requestor** – the employee or group submitting a technology request on behalf of a Business Unit.

4.23 **Run** – fourth (4th) and final stage of CREATe; defines IT Support using the Transition to Run Checklist for a request after it completes its Build stage and before it goes-live in test/production.

4.24 **Side-by-Side Upgrades** – refers to performing a congruent upgrade in both the original and a separate environment, saving the data, and then cutting over to the newer environment.

4.25 **Software Pilot** – the roll out of a new product (software) in real-world conditions to a small area of an organization to evaluate its viability.

4.26 **Support (Run) Team** – the group which operates, supports, and maintains a product or application.

4.27 **Systems Manager** – an IT manager who advises on and/or oversees aspects of system design, development, implementation, and post-implementation support; assigned to CREATe requests in Intake (by Requestor and BRM) to serve as [the] Project Manager for a solution.

4.28 **Transition to Run Checklist** – in-app checklist presented at the beginning of the Run stage (after completing Build); connects project team with IT groups to ensure requests are built to preserve system/data integrity, reliability, and user access security by promoting utilization monitoring and license adherence.

5.0 REQUEST TYPES & REQUIREMENTS – As per CEI CI-215, project registration with IT is mandatory for all technology-related projects. CREATe serves as the process to manage technical reviews of IT-related projects that meet one [1] or more of the following criteria:

a. Constitutes a change in IT architecture(s),
b. Constitutes a change in infrastructure design(s),
c. Includes the introduction of new or novel technology to Con Edison, and/or when
d. No applicable artifact is available on the EA SharePoint or ITPP Site

In short – any change in architecture, infrastructure, and/or introduction of new or novel technology should go through the CREATe process (excluding in-place and/or side-by-side upgrades).

5.1 CREATe Request Types & Requirements – See ***Appendix A, Table 1*** for a list of all CREATe Request types along with their (respective) ***Required Documentation*** (***Table 2)*** and ***Required Forms & Checklists (Table 3)***. ***Diagram 3, Workflows for CREATe Request Types***, illustrates the expected phases for each CREAT Request Type.

Consult the CREATe Requirements & Documentation Guide for more information and examples.

5.2 Exceptions – consult the CREATe FAQ page for any current exceptions.

6.0 PROCEDURE – CREATe involves the assessment of technical architecture and security features, as well as strategic alignment across the four CREATe stages of Intake, Review, Build, and Run. A CREATe request must also get approval for deployment through a different relevant funding process.

6.1 Intake – Intake is the initial stage in the CREATe process where requests are started by gathering the basic project information, assigning them to a BRM's portfolio of requests, and linking the request to its relevant Systems Manager. If no Systems Manager in IT matches the request, then a delegate (Band 3 or higher) from the requestor's organization will function as the Project Manager and take on the role of Systems Manager for the request. Business and/or IT leads can submit a new request via the CREATe Application as a requestor.

6.1.1 Accessing the App and CREATe Data – a link to the app is available here and on the IT Conor Page under the CREATe tile. A complete registry of requests will be stored on the CREATe SharePoint Site and can be accessed using the in-app PowerBI reports, "My Dashboard" or requested from a BRM or CREATe Admin.

6.1.2 Pending BRM, Pending Customer – after submitting a request, an IT Business Relationship Manager (BRM) examines the submission and the accompanying technical documentation to check that the request has all the relevant information needed to move to Review. The BRM may contact the requestor to find out more about the request if more information is required, which will change the status to "Pending Customer."

6.1.3 Pending Systems Manager – the BRM delegates the request to an IT Systems Manager (or Project Manager if there is no Systems Manager). The Systems Manager checks the documentation and the suggested solution before sending

the request for technical IT assessment during Review.

6.2 **Review –** Review, the second CREATe stage, sees that all requests are reviewed by the following IT groups:

- Enterprise Architecture (EA)
- Information Security (Cyber)

EA and Cyber conduct a parallel technical review of each request from their respective domains of expertise in the CREATe stage and provide a decision to proceed with the request after completion. The approval groups must follow data and network security protocols, architecture to corporate standards, and analytics standards to comply with CEI CI-215.

EA aims to understand how the request aligns with the company's technology roadmap and strategy, and how the system will interact with current in-service technology. For analytics initiatives, the EA Data Architect and Enterprise Data & Analytics Team will perform an extra layer of review.
Cyber Security ensures that the vendor and the solution do not compromise Company assets, information, networks, and other connected technologies. Cyber can mandate the completion of additional security scanning processes including:

1. Third-Party Risk Assessment (TPRA)
2. Third-Party Software Evaluation (TPSE)
3. Penetration (Pen) Testing
4. Privacy Impact Assessment (PIA)

6.2.1 **Pending EA/Cyber** – A request can only receive CREATe approval if it is approved by each individual group involved in the review process. Either of these two groups has the authority to reject the request, resulting in an overall rejection. The three potential outcomes of the review process are Approval, Rejection, or a request for additional information (Needs More Information, or NMI).

1. **Approval –** A request receives approval when the two relevant approval teams have approved it. Upon approval, the requestor is notified via an automated email, indicating that they may proceed with the project. This approval may be issued to the Supply Chain department to initiate any necessary purchases related to the approved request. In the event of any changes to the approved scope, the technical review teams must be notified for re-approval.

2. **Rejection –** A request may be rejected if any one of the approval groups involved in the review process rejects it. In such an event, the requestor will be notified of the rejection via an automated email. If the requestor wishes to continue pursuing the project, they must consider an alternative project scope or solution and resubmit it to the CREATe process for review. Cyber and EA Analysts will provide a justification and advise on recommendations for alternative options, if available.

3. **Needs More Information (NMI)** – In the event that any one of the approval groups requires additional information for proper review of a request, the request may be returned to the Business Relationship Manager (BRM) and Systems Manager for further review. The requestor will be notified via email that their request necessitates the provision of further information, such as documents or diagrams, to proceed.

CEI CI-215 gives the technical review teams final authority to approve technology based on IT guiding principles and standards. At the end of Review, all outstanding issues between the requestor and the review teams must be resolved.

6.3 **Build** – The Build stage, which is the third stage of the CREATe process, involves the collection of outputs and approvals from the Review stage to generate technical documents and timelines for the construction of a project system. The Systems Manager oversees the construction and delivery of the project. The Build stage ensures that approved technology requests adhere to established standards and do not deviate from reference architecture, blueprints, and design patterns.

6.3.1 **Readiness to Build Checklist** –During the Build stage of the CREATe process, the Readiness to Build Checklist is utilized to ensure that approved technology requests comply with established design standards and do not deviate from reference architecture, blueprints, and design patterns prior to proceeding to the Run stage.

The Readiness to Build Checklist, which replaces the Production Acceptance Checklist (PAC) Build portions, is the responsibility of the Systems Manager to complete the "Project Owner" section. The Systems Manager and Requestor are advised to contact IT Build groups identified in the Checklist sections for sign-off on questions related to their expertise.

A breakdown of which CREATe Request Types require a completed Readiness to Build Checklist before proceeding to Run can be found in ***Appendix 1, Table 3 of Required Forms & Checklists***. For assistance with Build & Run Checklist Navigation, please refer to *Appendix A, Diagram 1*.

6.4 **Run** – The Run stage, which is the fourth and final stage of the CREATe process, is responsible for defining the support for an approved request that has completed its Build stage. This stage is managed by the Systems Manager and the respective IT support groups. The transfer of knowledge from the Build stage to the Run stage ensures the maintenance of system integrity and reliability. The designated Run team for a request may be responsible for monitoring utilization and license adherence, while preserving data integrity and user access security.

6.4.1 **Transition to Run Checklist** – During the Run stage of the CREATe process, the Transition to Run Checklist is utilized to ensure the maintenance of system integrity and reliability, proper delegation of Run/Support teams, and preservation of data integrity and user access security prior to go-live.

The Transition to Run Checklist, which replaces the Production Acceptance Checklist (PAC) Run portions, is the responsibility of the Systems Manager (or

Project Owner from the business team) to complete the "Systems Manager" section. The Systems Manager and Requestor are advised to contact IT Run groups identified in the Checklist sections for sign-off on questions related to their expertise.

A breakdown of which CREATe Request Types require a completed Transition to Run Checklist before the request can go-live can be found in ***Appendix A, Table 3 of Required Forms & Checklists***. For assistance with Build & Run Checklist Navigation, please refer to *Appendix A, Diagram 1*.

6.5 **CREATe Request Close-Out** – It is important to retain the final email notification as a record of CREATe completion. This notification should be attached to any requisition(s) submitted to the Supply Chain department in instances where product or service procurement is necessary as part of the approved CREATe Request scope.

6.5.1 **For Projects and EPs –** CREATe workflow concludes after Transition to Run Checklist is completed.

6.5.2 **For PoCs and Pilots (Hardware/Software) –** CREATe workflow concludes after Transition to Run Checklist is completed. A new CREATe Request must be submitted as a follow-up in the case the PoC/Pilot is successful and wants to be pursued as a full Project.

6.5.3 **For RFPs –** CREATe workflow concludes after EA & Cyber Approval is received during Review. If a solution is chosen from a successful RFP, please submit a new CREATe Request for said solution as a Project, PoC, Pilot, or EP.

6.5.4 **For PowerApps –** CREATe workflow concludes after EA & Cyber Approval. Please log the new PowerApp in ServiceNow before go-live.

7.0 SUMMARY –

The CREATe process is a comprehensive and centralized system for the technical review of IT projects within Consolidated Edison Company of New York, Inc. (CECONY), Orange and Rockland Utilities, Inc. (O&R), and Con Edison Transmission, Inc. (CET). The process involves four stages: Intake, Review, Build, and Run, and ensures that all technology projects adhere to established standards and do not deviate from reference architecture, blueprints, and design patterns. Adherence to the CREATe process is essential for addressing the increasing reliance on information technology and mitigating cybersecurity threats.

8.0 RESPONSIBILITY –

8.1 The Director of IT Architecture & Digital Platforms has been granted authority to review and approve this document under CEI CI-215 for CECONY, O&R, or CET.

9.0 REFERENCES –

9.1 CEI CI-215 "Acquisition, Deployment and Support of Information Technology"
9.2 CREATe Requirements & Documentation Guide
9.3 CREATe SharePoint Portal
9.4 Software Development Lifecycle (SDLC) Guide

10.0 CHANGE LOG –

Date	Author	Version	Comments
3/22/2022	Owen Rosini	1.0	Initial instruction that references new CREAT Process (replacing TAP document ISPR2.0)
5/10/2023	Owen Rosini	1.1	Updated document for name change (CREATe) and additional stage details
7/28/2023	Owen Rosini	2.0	Added definitions and sections to reflect current CREATe expectations and standards
5/7/2024	Owen Rosini	2.1	Removed language in Sect. 5 regarding integrations, renamed title of procedure from “IT Project Registration” to “IT Technical Review”, phrasing changes, added summary and reference to SDLC

11.0 APPENDIX A – Support Tables and Diagrams

11.1 Table 1 – CREATe Request Definition Matrix (& Permitted Uses)

CREATe Type	Definition	Allowed to Integrate w/ Prod IT System	Allowed to Integrate w/ Test IT System	Used for Prod Operational Business Decisions?	Dev. Effort (Estimate)
Proof of Concept (PoC)	a trial intended to show that a design concept or business proposal is feasible for real-world deployment. PoC is successful, the solution *must* be resubmitted as a Project in CREATe for full review and consideration of production impact.	**No**	**No**	**No**	**Low**
Power App	a custom app that can be run on web/mobile platforms and is created in the PowerApps MS Application using low/no-code dev. tools. It can connect to data stored in 0365 sources (i.e., SharePoint, Microsoft 365, and SQL Server).	**Yes**	**Yes**	**No**	**Medium**
Software Pilot	the roll out of a new product (software) in real-world conditions to a small area of an organization to evaluate its viability. If a pilot is successful, the solution *must* be resubmitted as a Project in CREATe for full review and consideration of production impact.	**No**	**Yes**	**Yes**	**Medium**
Hardware Pilot	the roll out of a new physical product (hardware, sensor, IoT device, etc.) in real-world conditions to a small area of an organization to evaluate its viability. If a pilot is successful, the solution *must* be resubmitted as a Project in CREATe for full review and consideration of production impact.	**Yes**	**Yes**	**Yes**	**High**
Request for Proposal (RFP)	the evaluation of a vendor's product or contractor's ability to undertake a project started through the distribution of an RFP (business document that announces a project and solicits bids from qualified contractors to complete it) Once an RFP is complete, the chosen solution *must* be resubmitted as a Project in CREATe with final documentation and scope included for review.	**Yes**	**Yes**	**Yes**	**Medium**
Project	an individual or collaborative effort with a plan of action to produce a deliverable and/or achieve a particular goal	**Yes**	**Yes**	**Yes**	**High**
Enterprise Program (EP)	a collection of sub-projects managed as a group over an extended period to achieve efficiencies of scale for the business (i.e., CORE, GIS, REV) *EPs are funded at the Program Level (through the Rate Case)	**Yes**	**Yes**	**Yes**	**High**

11.2 Table 2 – CREATe Documentation Requirements Matrix

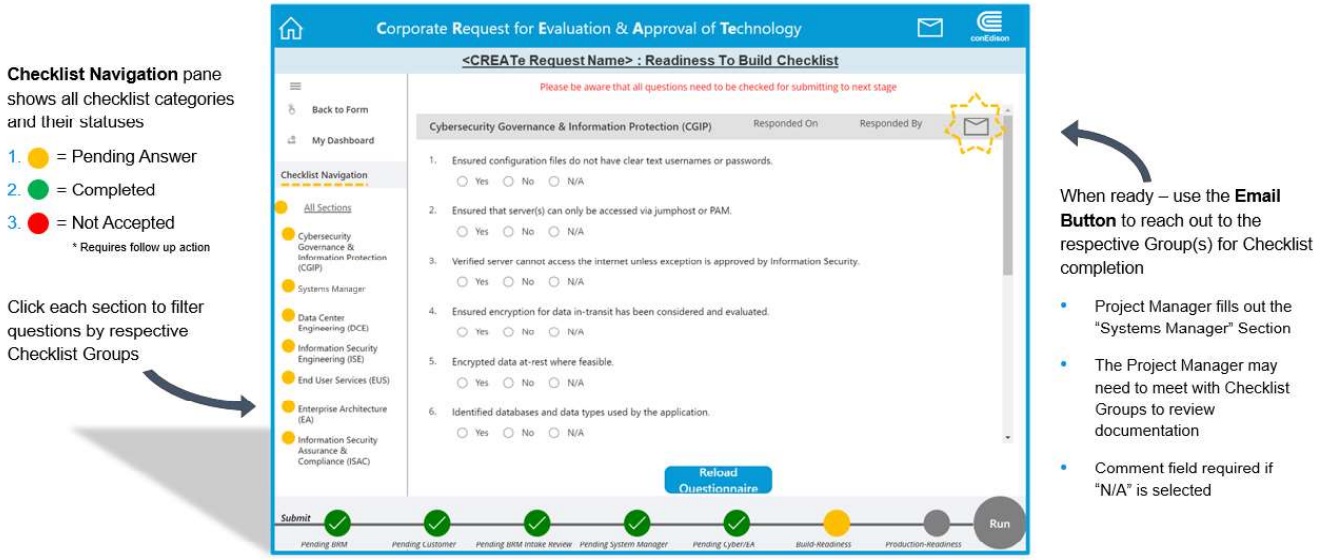
Document Type	CREATe Type						
	PoC	PowerApp	Software Pilot	Hardware Pilot	RFP	Project	EP
Project Objective	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Network / Infrastructure Diagram	Yes	No	Yes	Yes	No	Yes	Yes
Data Flow Diagram	No	Yes	Yes	Yes	No	Yes	Yes
High Availability & Disaster Recovery Strategy	No	No	No	No	No	Yes	Yes
Support Model	No	No	No	No	No	Yes	Yes

11.3 Table 3 – CREATe Form & Checklist Requirements Matrix

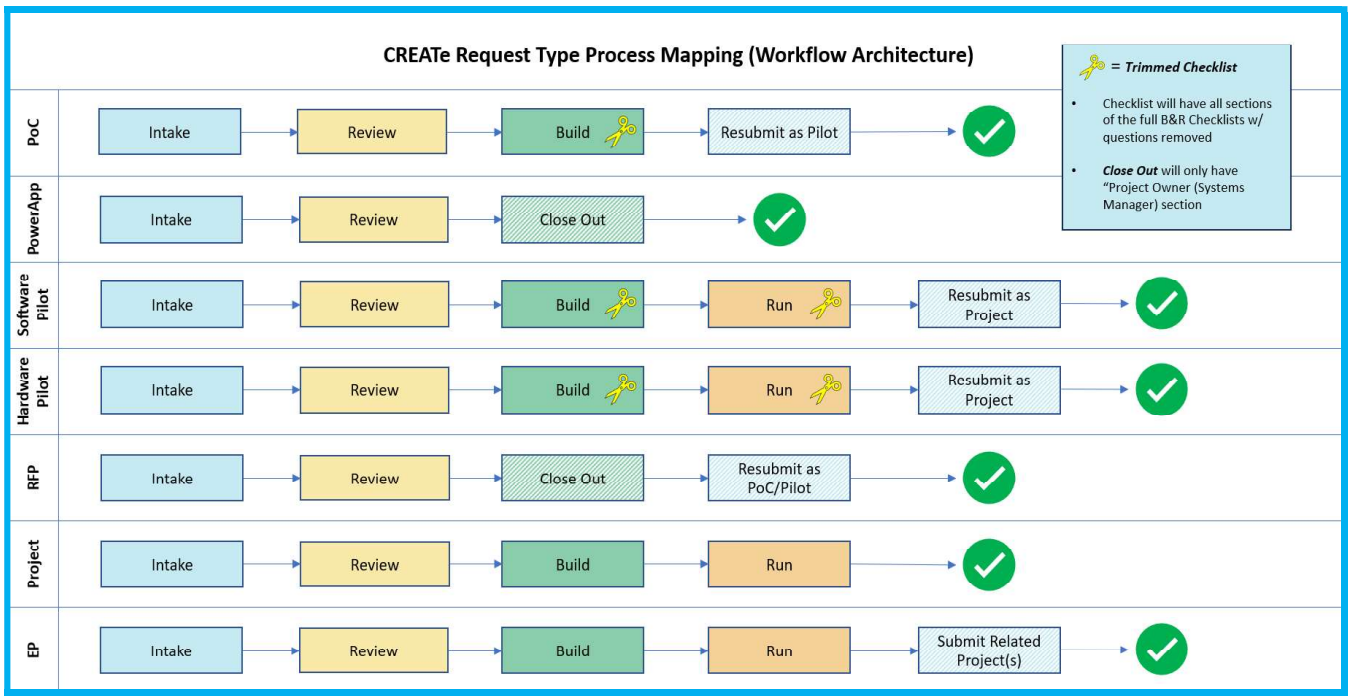
Form / Checklist Name	CREATe Type						
	PoC	PowerApp	Software Pilot	Hardware Pilot	RFP	Project	EP
Cyber Security Questionnaire 2.0	Yes	No	Yes	Yes	No**	Yes	Yes
Third Party Risk Assessment (TPRA)	Yes*	No	Yes*	Yes*	No**	Yes*	Yes*
PII/PIA Form (Find Link in Email Notification)	Yes^	Yes^	Yes^	Yes^	Yes^	Yes^	Yes^
Power App Detail Form	No	Yes	No	No	No	No	No
» Readiness to Build Checklist	Yesº	No	Yes	Yes	No	Yes	YesT
» Transition to Run Checklist	Yesº	No	Yes	Yes	No	Yes	YesT

^ = Required only if project touches PII/PHI data
** = Required unless selected vendor is known
* = Required only when data is being stored or sent to a third-party vendor
º = Consult Build and/or Run Team(s) to determine N/A sections
T = Use EP Build & Run Checklist Template

11.4 Diagram 1 – Build & Run Checklist Navigation



11.5 Diagram 2 – Workflows for CREATe Request Types



Attachment 3

CEI 311 : AI Corporate Policy Statement

AI Guidelines

Gen AI Technology Playbook

Governance Tiered Standard

conEdison, inc.

Corporate Policy Statement

SUBJECT

CEI-311 Consolidated Edison, Inc. AI Policy

1.0 PURPOSE -- This Policy (a) communicates our commitment to responsible and ethical AI development and use, and (b) provides a framework to govern Con Edison AI activities.

2.0 APPLICATION -- This Policy applies to all employees and contractors of Consolidated Edison, Inc. (CEI) and its subsidiaries, including Consolidated Edison Company of New York, Inc., Orange and Rockland Utilities, Inc (O&R), and Con Edison Transmission. It includes any stage in the AI use case life cycle for AI Systems developed internally, acquired from third parties, embedded within vendor products, or accessed through external platforms for Company business purposes.

3.0 GENERAL PROVISIONS --

3.1 Definitions -

Artificial Intelligence (AI) - AI includes machine learning, generative AI, large language models, predictive analytics, and other technologies that autonomously or semi-autonomously analyze data, generate content, make recommendations, or support decision-making.

AI System - Any software, model, tool, or service incorporating AI functionality used in connection with Company business, including Agentic AI and Generative Artificial Intelligence (Gen AI).

AI Agent/Agentic AI - A software construct that autonomously or semi-autonomously plans, orchestrates, or executes actions across one or more AI models, tools, data sources, or systems over time, with limited human intervention. For example, Agentic AI can make decisions and take actions in digital environments.

AI Governance Tier - The Company's classification assigned to an AI System based on its intended use, potential impact, and data characteristics. AI Governance Tiers establish the required governance processes, controls, oversight activities, and approvals necessary for responsible development, deployment, and operation of AI Systems.

Artificial Intelligence (Generative AI / Gen AI) - A class of artificial intelligence technologies designed to generate new, original content — including, but not limited to text, images, audio, video, software code, and synthetic data in response to user-provided prompts. These systems are trained on datasets to recognize patterns, relationships, and structures, allowing them to produce outputs that mimic human creation rather than simply analyzing or classifying existing data.

Large Language Model (LLM) - An AI System can be trained using large volumes of data to recognize patterns in language and generate human-like responses to prompts. An LLM produces output (e.g., text, code, images, audio) by predicting what is most appropriate given the input it receives. LLMs can perform a wide range of natural language tasks, including text generation, summarization, translation, classification, and code drafting, in response to user-provided prompts.

AI Use Case – A defined business or operational application of an AI system intended to achieve a specific objective, outcome, or capability. AI use cases shall be assessed through the Company's project registration and governance processes in accordance with CEI-215 when they involve the development, acquisition, implementation, integration, enhancement, or material modification of an AI System.

3.2 Responsible AI Principles –
The Responsible AI Principles define the expectations that guide responsible behavior and decision-making when designing, using, and relying on AI across the Company. They promote human accountability, risk awareness, and use aligned with Company values throughout the AI lifecycle and are based on the National Institute of Standards and Technology's (NIST) AI Risk Management Framework characteristics of trustworthy AI Systems.

a. **Know and Follow the Law**
All users must comply with legal considerations, including, for example, privacy and data protection, intellectual property and copyright, employment, and regulatory obligations. Only use Company-approved AI Systems.

b. **Transparency and Explainability**
AI use must be transparent. The role of AI, including its influence on decisions, and relevant data or model characteristics, must be appropriately documented and communicated in a manner proportionate to risk and impact. Where possible, based on computing system constraints, content initially generated using AI tools must be clearly labelled using an explicit indication (i.e., "AI-Generated Content" or "Generated Using AI").

c. **Human Oversight ("Human in the Lead")**
Human accountability shall be maintained throughout the AI lifecycle through human oversight appropriate to the risk and impact of the AI System or Use Case. The Company may apply different oversight models to achieve this objective; however, responsibility for decisions, actions, and outcomes shall

remain with individuals, not AI Systems. AI cannot replace critical thinking skills, or human review.

d. **Monitoring for Accuracy**
Content generated with AI is not always accurate. Generative AI Systems can produce inaccurate and fictitious answers that seem legitimate. Any AI-generated content must be regularly monitored, evaluated, reviewed, and maintained by the owner to confirm it is providing accurate, and reliable results, including fact checking and proofreading, for their intended use. AI outputs must not be treated as authoritative without appropriate validation.

e. **Fairness and Oversight**
AI outputs may be influenced by biased or flawed data, potentially resulting in implicit biases, unfair practices, or discriminatory outcomes. These concerns are particularly heightened when AI is used to screen applicants or candidates for hiring or promotion, evaluate qualifications or performance, or determine compensation. Project teams must actively evaluate and mitigate bias risk throughout the AI lifecycle.

f. **Accountability**
Clear ownership, defined responsibilities, and auditability must be established so that employees and system owners—not AI Systems—remain accountable for decisions, actions, and outcomes. Individuals using AI Systems are responsible for the results they produce.

g. **Privacy and Data Protection**
Approved AI Systems must be contractually obligated to protect information, including relating to people, customers, employees, critical infrastructure, and sensitive data through appropriate safeguards, minimal and purpose-limited data use, secure handling, and compliance with applicable data classification and privacy laws and regulations.

h. **Safety and Security**
Approved AI Systems must be designed, deployed, operated, and monitored to protect the safety of individuals, the security of Company systems and data, and the integrity of business and operational processes. Safeguards and controls shall be proportionate to the risk and impact of the AI System or Use Case.

3.3 <u>AI Use Considerations</u> -

- Use only Con Edison's approved AI Systems. The list of approved AI tools and platforms is found at PB.ADM.02 - Gen AI Technology.
- Before use or deployment,
  - Vendor and supplier use of AI Systems, provision of AI-enabled services, or implementation of AI functionality (even within a previously approved AI System) must be approved through Enterprise Architecture and the Company's Third-Party Risk Management program as well as be certified or recertified through the CREAT program under CEI 215 and follow appropriate Supply Chain processes.
  - Where appropriate or required by law, Customers should be advised regarding the use of customer information in approved AI Systems.

3.4 Prohibited Uses of AI -

The following uses of AI, unless specifically authorized by the Executive AI Governance Committee, are prohibited.

- Undisclosed AI-generated communications presented as human-authored in regulatory or customer contexts.
- AI-based social scoring of customers or employees. (Social scoring is the practice of evaluating, ranking, or assigning a score to individuals based on, for example, their behavior or characteristics, and using that score to make decisions about their access to opportunities, services, benefits, or rights.)
- Automated employment decision making tools that substantially assist or displace discretionary decision making (that is, for example, relying on an output score without other factors), for decisions related to hiring, firing, discipline or promotions.
- Automated consequential decision-making that directly affects customer, operations, individuals' rights, access to services, financial outcomes, or safety—that are made without human review before the decision takes effect.
- With the exception of use by Corporate Security for Insider Threat purposes, emotion recognition technologies used for employment decisions.
- Deployment of AI systems that materially affect Safety-Critical Systems that are not compliant with this Policy's principles on Human Oversight and

Accountability Using Generative AI in violation of any contract terms and conditions, including the terms and conditions applicable to AI that are included in contracts.

3.5 AI Governance Committee Framework -

Con Edison's responsible AI strategy and governance framework includes three tiers of committees. Together, these three tiers provide the support and framework for the Companies' AI projects. The three tiers and their respective functions are:

- AI Executive Oversight Committee – Provides oversight and strategic guidance for the Company's use of AI, reinforcing responsible and compliant AI use through leadership expectations and accountability.

- AI Operating Group – VP-level body verifies adoption and enforcement of AI governance standards across functions, contributes to governance reporting, and escalates risks and non-compliance.

- AI Governance Working Group – Operational body responsible for implementing and operating AI governance controls, including risk classification, standards, and lifecycle checkpoints and maintains visibility into compliance and control adherence.

3.6 Governance Tiering -

All AI Systems shall be assigned a Governance risk tier through the Company's AI Governance Tiering Framework. Governance tiering shall be performed through the **C**orporate **R**equest for **E**valuation & **A**pproval of **Te**chnology (CREATe) or similar process during project registration in accordance with CEI 215. The controls for the AI systems and use cases are defined by tier level. There are 4 Governance Tiers under which each project will fall in terms of controls and review level. The review will consider factors such as intended use, potential impact, data sensitivity, regulatory considerations, and organizational context.

- **Tier 1** – Standard Approval: AI Systems with limited operational impact that support internal productivity and do not influence consequential business, customer, safety, or regulatory decisions. Example: Drafts internal content for employee review using an approved enterprise tool.

- **Tier 2** – Approval with Conditions: AI Systems that support business processes, customer interactions, or operational decision-making and require

enhanced governance oversight. Example: Analyzes operational data and recommends actions requiring human validation.

- **Tier 3** – Active Oversight: AI Systems that impact customers, employees, reliability, safety, regulated activities, or other business-critical functions and require formal governance review and ongoing oversight. Example: Supports customer, reliability, safety, or regulatory decisions under active oversight.

- **Tier 4** – Executive Determination: AI Systems presenting significant enterprise, legal, regulatory, ethical, reputational, or control considerations that require senior executive review and determination prior to implementation. Only the AI Executive Governance Committee can approve a Tier 4 project. Example: Initiates or materially influences decisions with significant enterprise implications.

Any use of the systems must comply with the required controls.

3.7 AI Issues Reporting and Escalation -

Potential AI misuse resulting in ethical risks, compliance issues or potential data incidents, such as unauthorized data access or leakage, determined biases or hallucinations affecting decisions or outputs used in error for external communications, must be reported promptly through established Company channels. This includes handling AI-related incidents in accordance with CI-260-4, Corporate Response to Incidents and Emergencies.

4.0 Responsibilities

AI Executive Oversight Committee

- Provides oversight and strategic guidance for the Company's use of AI, reinforcing responsible and compliant AI use through leadership expectations and accountability.

AI Operating Group

- VP-level body verifies adoption and enforcement of AI governance standards across functions, contributes to governance reporting, and escalates risks and non-compliance.

AI Governance Working Group

- Operational body responsible for implementing and operating AI governance controls, including risk classification, standards, and lifecycle checkpoints and maintains visibility into compliance and control adherence.

Business Owner

- Executive in the business unit who is accountable for the use-case's purpose, benefits, risks and results.
  i. Signs off before go-live.
  ii. Remains accountable for any decision the AI supports.

Technical Owner

- Responsible for the system's technical behavior.
  i. Development, configuration, and testing.
  ii. Monitoring performance and drift.
  iii. Change control and documentation.

All employees

- Use only approved tools.
- Review outputs to confirm accuracy and appropriateness of outputs.
- Keep confidential and customer data out of tools not approved to handle confidential and/or customer data.
- Report misuse.

Cybersecurity: assesses AI-specific threats such as prompt injection and data poisoning, and reviews security before deployment.

Privacy: approves the use of personal and customer data, checks data quality and lineage, and sets retention rules.

Legal / Regulatory / Compliance: provides advice on legal obligations associated with AI use, including, for example, regulatory requirements, necessary contract terms and intellectual property.

Procurement / Third-Party Risk: In collaboration with ETS TPRA, Supply chain TPRM program, evaluates AI-related risks associated with third-party products and services, including vendor controls, contractual protection, data handling practices, and safeguards governing the use of company data for AI model training or other purposes.

5.0 <u>References</u> – This Policy has been drafted in reference to and alignment with the following internal and external policies and guidelines:

- NIST AI Risk Management Framework (AI 100-1)
- ISO/IEC 42001
- CEI-211 CI Protection of Personally Identifiable Information (PII)
- CEI-407 Data Classification
- CEI-408 Protection of Critical Energy Infrastructure Information
- CEI-215 CI Acquisition, Deployment, and Support of Information Technology
- AI Guidelines (AI Technology Guidelines and Supporting Standards)
- 260- 4 CI Corporate Response to Incidents and Emergencies
- Con Edison Code of Ethics and Business Conduct
- For legal guidance related to AI use, including AI applications involving applicants or employees, contact the Law Department AI Committee at, dl-LawdeptAIcommittee@coned.com

6.0 Advice and Counsel – The Senior Vice President & Chief Information Officer and Senior Vice President and General Counsel will provide advice and counsel on this Corporate Policy Statement.

7.0 Policy Owner – The Senior Vice President and Chief Information Officer owns this Corporate Policy Statement.

8.0 Review Cycle – This Corporate Policy Statement shall be reviewed annually, or upon any material change in applicable regulation, Company AI strategy, or governance structure, whichever occurs first.

9.0 Summary of Changes –

APPROVED DATE	SUMMARY OF CHANGES
November 6, 2026	• This is a new corporate policy.

Corporate Guideline

SUBJECT

AI Guidelines

BingChatEnterprise Responsible Use Guidelines

Generative Artificial Intelligence (AI) can revolutionize business processes by increasing efficiency, improving accuracy, and reducing costs. However, there are significant practical, ethical, and legal considerations that must be carefully evaluated so that employees appropriately use AI and comply with applicable laws and regulations.

Microsoft has recently made a protected version of BingChatEnterprise available to the Company. This product uses the ChatGPT-4 engine but prevents any proprietary information from entering the public domain. **BingChatEnterprise is the only permissible form of generative (Chat GPT-type) Artificial Intelligence that may be used for Company work**. Employees may however use AI functions that are built into Company systems.

These Guidelines apply to all employees and contractors of Con Edison.

Employees must not upload, disseminate, or otherwise provide AI tools other than BingChatEnterprise with restricted or confidential information or data (see CEI-407 Data Classification) including information related to the Company, employees, contractors, customers, or vendors.

To protect the Company, our customers, employees, and shareholders, here is what you must do:

- **Use Only Con Edison's BingChatEnterprise for AI.** If you are properly logged into BingChatEnterprise, you will see your picture with your name and the words: "Protected." If this information is not on the screen, you are not using the proper product and you should not perform any Company work using that AI source.

- **Respect the law.** Use of BingChatEnterprise must comply with legal considerations, including, for example, privacy and data protection, intellectual property, and copyrights. Follow all existing Company technology and other policies, see Policies & Procedures - Home (sharepoint.com).

APPROVED	APPROVED DATE	LAST REVIEWED DATE	NUMBER	SUPERSEDES	PAGE 1 OF
Mary Kelly	09/28/2023	9/28/2023	000-1	NEW	2 PAGES

- **Transparency:** For transparency, all initial BingChatEnterprise-generated content must be clearly labeled manually through a Watermark on the entire document (e.g., labeled as "AI GENERATED CONTENT"). The watermark can be removed in subsequent versions but a copy of the original must be maintained.

- **Monitoring for Accuracy.** Any BingChatEnterprise-generated content should be regularly monitored and evaluated by the business system owner to confirm that it is providing accurate and reliable results. Such monitoring includes fact checking and proofreading. The data and information in BingChatEnterprise includes real-time data.

- **Starting point, not the finished product.** BingChatEnterprise-generated content should be viewed as a starting point, not the finished product. While AI can provide a valuable tool for generating content, it cannot replace the creativity and critical thinking skills of humans.

- **Fairness and Oversight:** BingChatEnterprise output may be based on historical data and the results potentially may contain implicit biases, unfair practices or can provide discriminatory results. These concerns are particularly heightened when AI is used to screen applicants or candidates for hiring or promotion, evaluate qualifications or performance, or determine compensation. Specific laws currently exist that touch upon this issue. Please reach out to the appropriate Legal or Compliance partner for additional guidance if your use of AI may impact an applicant or employee.

What not to do?

- Do not use any other form of AI to perform Company work, including any public-facing version of ChatGPT, as this product does not restrict public access to our proprietary data.

Report concerns appropriately. If you feel that anyone in or associated with Con Edison has been or will be engaged in any conduct that may be in violation of these Guidelines or Company policy, please discuss your concerns with your supervisor, or any of the following resources: Business Ethics and Compliance, and/or Diversity, Equity and Inclusion, as relevant.

conEdison

Corporate Guideline

SUBJECT

AI Guidelines

Artificial Intelligence (AI) Responsible Use Guidelines

Introduction

Artificial Intelligence (AI) can revolutionize business processes by increasing efficiency, improving accuracy, and reducing costs. However, there are significant practical, ethical, and legal considerations that must be carefully evaluated so that employees appropriately use AI and comply with applicable laws and regulations. These Guidelines apply to all employees and contractors of Consolidated Edison, Inc.

AI Governance

The Company's AI Governance Framework includes a cross-functional AI Governance Committee to oversee AI-related activities and establish overall accountability for our use of AI, inclusive of approvals associated with the use of any AI tool or system within the organization. The AI Governance Committee shall be comprised of representatives from Enterprise Data & Analytics, Information Security, Enterprise Architecture, Privacy Compliance and Law. The AI Governance Committee will assess the potential practical, security, ethical, regulatory, and legal use of any AI system and provide guidance, recommendations, and final approval for using any AI system or AI-enabled technology.

Requirements:

- Any AI tool or system must receive approval through the CREATe Project Registration process (see CEI-215 CI Acquisition, Deployment, and Support of Information Technology).

- Vendors and suppliers using, providing, or adding AI functionality, even within a previously approved system, must be vetted and approved through Supply Chain Management's Third Party Risk Management process as well. The contract must include terms provided by Law that discuss the AI usage and provide appropriate protections.

- All generative AI tools that have not been approved will be blocked. Information Security will maintain a record of blocked sites as well as any requests for exceptions to access these sites.

- Enterprise Architecture will maintain a list of approved AI tools and platforms. (see PB.ADM.02 - Gen AI Technology.pdf)

Use of Generative AI

Some Generative AI Providers (i.e. developers, vendors) have made protected versions of their tools available to the Company. These products use modern engines but prevents any proprietary information from entering the public domain. **The approved list of tools are the only forms of generative (ChatGPT-type) Artificial Intelligence that may be used for Company work.**

Employees must not upload, disseminate, or otherwise provide restricted or confidential information of data (see CEI-407 Data Classification) to any AI tools other than the IT-approved list of tools, inclusive of any information related to the Company, employees, contractors, customers, or vendors.

To protect the Company, our customers, employees, and shareholders should adhere to the following guidelines:

- **Use Only Con Edison's Approved AI Platforms.**

- **Respect the law.** Use of approved Generative AI tools must comply with legal considerations, including, for example, privacy and data protection, intellectual property, and copyrights.

- **Transparency.** For transparency, all content initially generated using Microsoft CoPilot or any other approved AI platform must be clearly labeled using an explicit indication (e.g. labeled as "AI GENERATED CONTENT").

- **Human oversight ("Human in the Loop").** All use of Generative AI must be subject to human oversight so that tool usage complies with the Policy and the Company's Standards of Business Conduct. You may not use AI to fully automate business processes or as a substantial factor in making a consequential decision without direct human oversight.

- **Monitoring for Accuracy.** Any AI-generated content must be regularly monitored and evaluated by the business system owner to confirm it is providing accurate and reliable results. Such monitoring includes fact checking and proofreading.

- **Starting point, not the finished product.** AI-generated content must be considered as a starting point, not the finished product. AI cannot replace human creativity and critical thinking skills.

- **Fairness and Oversight.** Generative AI outputs may be influenced by biased or flawed input data, potentially resulting in implicit biases, unfair practices, or discriminatory outcomes. These concerns are particularly heightened when AI is used to screen applicants or candidates for hiring or promotion, evaluate qualifications or performance, or determine compensation. Since specific laws address this issue, please reach out to dl-LawdeptAIcommittee@coned.com for additional legal guidance if your AI use impacts an applicant or employee or for other legal questions associated with AI use.

- **Report concerns appropriately.** If you feel that anyone in or associated with Con Edison has been or will be engaged in any conduct that may be in violation of these Guidelines or Company policy, please discuss your concerns with your supervisor, or any of the following resources: Business Ethics and Compliance Helpline, and/or Diversity, Equity and Inclusion, as relevant. If you have any suspicion of data loss, contact PII Incident Response Team, piiincidentresponseteam@coned.com.

What not to do?

- Do not use any form of Generative AI outside of approved platforms and tools, as these products may not restrict access to our proprietary data.

Any AI related questions should be sent to: dl-ITGenAIIntake@coned.com.

Generative AI Technology

Playbook

Authored and published by
IT Enterprise Architecture

AUTHOR	APPROVED	DATE	VERSION	SUPERSEDES	PAGE
Gihan Haenlein Francesco Ciulla Joseph DeMarco	ARB	9/30/2026	2.1	N/A	1 of 9

Table of Contents

1. PURPOSE 3
2. GENERATIVE AI 3
3. APPROVED GENERATIVE AI TECHNOLOGIES 4
4. REFERENCE & RESOURCES 8
5. CHANGE LOG 9

1. PURPOSE

To list approved Generative AI technologies from IT, published on the EA Portal, ETS-EA - Home.

If you have any questions about the guidelines and approved Gen AI technologies, please email the Enterprise Architecture group at dleaitarchitecture@coned.com.

2. GENERATIVE AI

Generative AI(GenAI) is a type of artificial intelligence (AI) that creates new content such as text, images, video, audio, or software code. It relies on advanced machine learning models, which simulate the learning and decision-making process of the human brain. The models learn patterns and structures from vast amounts of data and use this knowledge to generate new content.

a. Users can directly interact with GenAI tools, such as Microsoft 365 CoPilot, by entering prompts through a process known as prompt engineering.

   i. Any new GenAI tool must undergo the CREATe approval process prior to being utilized.

b. Vendor software with embedded GenAI capabilities adds generative AI functionality to existing applications. This enhancement boosts the software's overall functionality and provides convenient, context- specific generative capabilities within the current framework.

   Con Edison has established guidelines for handling GenAI features within vendor applications:

   i. **New applications with GenAI Capabilities** must go through the CREATe process for a detailed review of the AI component.

   ii. Approved Applications with Gen AI functionality:

   - **Disable Option Available for GenAI Feature:** If the embedded GenAI feature can be disabled, it must remain disabled until an in-depth review of the AI component is completed. This review is conducted through the CREATe process, ensuring that the AI solution meets all necessary criteria before being activated

   - **No Disabled Option Available for GenAI Feature:** If the embedded GenAI feature does not have a disable option, an in-depth review of the AI component must be completed via the CREATe process prior to activating or utilizing that component. This ensures that the AI solution is thoroughly evaluated for safety, effectiveness, and compliance before being implemented in the application.

3. APPROVED GENERATIVE AI TECHNOLOGIES

Due to the nature of Gen AI technology, updates or amendments will be made to this list in accordance with innovative technologies, security protections, regulatory requirements, and corporate policies.

a. Microsoft Office 365 Copilot

Microsoft Copilot is an AI-powered assistant designed to help users with a wide range of tasks. It leverages advanced language models to provide support in productivity, creativity, and information retrieval.

The list below is not exhaustive but contains base examples of Microsoft products that integrate with Copilot.

Microsoft Copilot integrates seamlessly with the following Microsoft 365:

i. **Microsoft Word**: Copilot helps you draft, edit, and summarize documents, making writing tasks more efficient.

ii. **Microsoft Excel**: It assists in analyzing data, creating visualizations, and generating insights, simplifying complex data tasks.

iii. **Microsoft PowerPoint**: Copilot aids in designing presentations, suggesting layouts, and creating content, helping you deliver impactful presentations.

iv. **Microsoft Outlook**: It can summarize long email threads, draft responses, and manage your inbox more effectively.

v. **Microsoft Teams**: Copilot enhances collaboration by summarizing meetings, generating action items, and facilitating communication.

b. Microsoft Dynamics 365 Copilot

Microsoft Dynamics 365 Copilot is an AI-powered assistant integrated into Microsoft Dynamics 365 applications. It enhances productivity and efficiency across various business functions by providing interactive, AI-driven assistance.

Microsoft Dynamics 365 Copilot integrates seamlessly with the following:

i. **Power Apps:** Copilot feature in Power Apps leverages AI to assist users in building and managing applications more efficiently. It provides capabilities such as natural language to code, AI-powered suggestions, and data processing.

ii. **Power Automate**: Copilot integration allows users to leverage AI-driven automation capabilities within their Dynamics 365 environment. Copilot in Power Automate helps streamline workflows

by using natural language to create and refine cloud flows, assist in data ingestion for process mining, and analyze automation activities.

iii. **Microsoft Copilot Studio:** Microsoft Copilot Studio is a low-code platform for building, customizing, and testing AI agents and chatbots that connect to Microsoft and third-party data sources, automate workflows, and take actions across enterprise systems, all within the Microsoft 365 and Power Platform ecosystem.

c. Microsoft GitHub Copilot

Microsoft GitHub Copilot is an AI-powered coding assistant developed by GitHub, OpenAI, and Microsoft. It helps developers write code faster and with less effort by providing contextual suggestions and code completions directly within their integrated development environments (IDEs) like Visual Studio Code.

d. Microsoft Edge Copilot Enterprise

Microsoft Edge Copilot Enterprise is an AI-powered feature integrated into the Microsoft Edge browser, designed to enhance productivity, and provide enterprise-level data protection.

e. Microsoft Azure AI

Microsoft Azure AI is a comprehensive suite of artificial intelligence (AI) services and tools offered by Microsoft through its Azure cloud platform. It enables developers and organizations to build, deploy, and manage AI solutions at scale.

f. Google Gemini Enterprise

Google Gemini Enterprise is an AI-powered assistant designed to help users with a wide range of tasks across productivity, creativity, and information retrieval. It uses Google's advanced large language models to deliver intelligent, context-aware assistance within enterprise environments, with built-in data protection and compliance controls suited for organizational use.

The list below is not exhaustive but contains base examples of Microsoft products that integrate with Gemini Enterprise.

Google Gemini Enterprise integrates seamlessly with the following Microsoft 365:

i. Azure Active Directory: Gemini integrates with Azure AD to support identity-aware experiences, ensuring access and personalization align with each user's organizational profile.

ii. Microsoft OneDrive: Gemini can access and reference files stored in OneDrive, enabling users to interact with and generate content based on their existing documents.

iii. Microsoft Outlook: Gemini integrates with Outlook to help users summarize emails, draft responses, and manage communication more efficiently.

iv. Microsoft SharePoint: Gemini can connect to SharePoint to surface and interact with organizational content stored across SharePoint sites.

v. Microsoft Teams: Gemini enhances collaboration within Teams by supporting communication workflows and providing AI-driven assistance directly within the Teams environment.

g. Gemini Enterprise Agent Platform

Gemini Enterprise Agent Platform is a comprehensive suite of artificial intelligence services and tools offered by Google through its Google Cloud platform. It enables developers and organizations to build, deploy, and manage AI solutions at scale. Vertex AI provides access to Google's foundation models, including the Gemini model family, along with tools for fine-tuning, grounding, and orchestrating AI workflows across enterprise applications.

h. EddyGPT (Every Day Discover Your Greatest Potential Together)

EddyGPT is a secure, in-house generative AI assistant developed by Con Edison. It is designed to provide employees with conversational, prompt-based AI capabilities similar to ChatGPT, enabling content generation, summarization, and knowledge support within the corporate environment. It serves as the approved enterprise alternative to public AI tools, aligning with Con Edison's cybersecurity policies, data protection requirements, and Responsible AI standards.

EddyGPT delivers a unified user experience across multiple foundation models from providers such as OpenAI, Google Gemini, and Anthropic Claude, accessed through Azure Foundry and Google Vertex AI. Users can select the model best suited to their use case and adjust parameters such as reasoning depth and temperature.

The platform is available to all Con Edison employees and contractors on the corporate network without individual licensing. It operates on a centrally managed, consumption-based model that enables scalable, cost-controlled access.

EddyGPT supports a range of business and technical use cases, including:

- Drafting and refining internal communications
- Summarizing documents, advisories, and reports
- Assisting with knowledge article and technical documentation creation
- Supporting development workflows such as code generation, debugging, and prototyping

- Enabling non-technical users to automate workflows, build dashboards, and create tools through natural language

Additional capabilities include multi-file ingestion and analysis, allowing users to upload and process PDFs, spreadsheets, code, and images within a conversational context.

EddyGPT is architected with enterprise-grade security and governance controls, including network-restricted access, content filtering, prompt injection protections, and strict data handling practices. Prompts are transiently processed and are not stored or used for model training, ensuring that user data remains within the enterprise boundary.

Here is the link to EddyGPT: **Eddy | Your everyday AI pal**

i. SPARK AI (Smart Precise Answers Relevant Knowledge)

SPARK is a Con Edison–developed generative AI platform that enables users to build and interact with custom AI assistants (agents) through a no-code interface. Built on a retrieval-augmented generation (RAG) architecture, SPARK allows users to create knowledge-driven AI solutions by uploading enterprise documents and querying them through natural conversation, with citations linked directly to source content.

SPARK provides an intuitive interface for defining agent instructions, configuring models, and managing knowledge sources, making it accessible to both technical and non-technical users. Core capabilities include document analysis, knowledge base search, summarization, and conversational interaction, supporting business use cases such as contract interpretation, document comparison, and knowledge navigation.

SPARK integrates seamlessly with the following:

- **Knowledge Sources:** Users can upload enterprise documents (PDFs, Word, spreadsheets, and similar formats) as grounded knowledge for custom agents, with responses anchored by integrated citations.
- **Azure AI Services:** SPARK leverages Azure Functions, Azure Search, and chat completion APIs to deliver scalable retrieval and generation workflows.
- **Custom Agent Deployment:** Users can create, configure, and deploy purpose-built knowledge assistants for individual, team, or enterprise use.

Here is the link to SPARK: SPARK AI

j. CELINE (Con Edison Listening Intelligence Next Engine**)**

CELINE is a Con Edison–developed generative AI solution designed for automated call transcription and analysis. It transforms the manual review of customer interactions into scalable, AI-driven insights, supporting customer-facing and operational teams that handle large volumes of call data.

CELINE processes audio recordings, including call center interactions and voicemails, by combining speech-to-text and generative AI technologies. Users can upload audio files, transcribe conversations with speaker identification, and analyze interactions to produce structured summaries, evaluations, and actionable recommendations.

CELINE is built on an Azure-based AI stack, leveraging Azure OpenAI services for natural language analysis and Azure Whisper for transcription, combined with scalable processing and web-based interfaces to support both real-time and batch workloads.

CELINE operates within Con Edison's enterprise environment and aligns with Enterprise Architecture governance, cybersecurity policies, and Responsible AI standards, ensuring secure handling of sensitive operational data.

CELINE supports the following core capabilities:

- **Transcription:** High-accuracy speech-to-text with speaker identification, powered by Azure Whisper.
- **AI Analysis:** Structured summaries, evaluations, and recommendations generated through Azure OpenAI services.
- **Reporting:** Automated, executive-ready outputs (e.g., PDF reports) for operational decision-making.
- **Interactive Querying:** Conversational interaction with analyzed content, including call comparison and template-based evaluation.

Here is the link to CELINE: CELINE - Intelligent Call Analysis

4. REFERENCE & RESOURCES

- Add Enterprise data as a knowledge source - Microsoft Copilot Studio Learn
- Introduction to connectors and data stores - Gemini Enterprise
- Copilot in Power Apps overview - Power Apps | Microsoft Learn

5. CHANGE LOG

Date	Version	Description	Author	Approved By
12/17/24	1.0	Initial Document	Gihan Haenlein Francesco Ciulla Joseph DeMarco	ARB
01/28/26	1.0	No Updates, Approved for 2026	Gihan Haenlein Francesco Ciulla Joseph DeMarco	ARB
5/21/26	2.0	Added Google Gemini, Gemini Enterprise Agent Platform, EddyGPT, SPARK, CELINE	Gihan Haenlein	ARB
8/26/26	2.1	Removed references to the GenAI pre-intake process	Gihan Haenlein	ARB

Purpose

This standard defines the minimum required governance controls for AI systems based on assigned governance tier. Controls are intended to support consistent, risk-based oversight of AI systems throughout their lifecycle.

Higher governance tiers may require enhanced governance, documentation, testing, monitoring, oversight, and approval activities proportional to the system's potential impact and risk exposure.

Control Requirement Terminology

To support consistent interpretation and application of controls across the framework, the following standardized requirement terms are used throughout this document:

- **Not Required**: The control is not mandatory for the specified governance tier. Teams may implement the control voluntarily based on business needs, operational considerations, or governance recommendations.
- **Conditional**: The control may be required depending on factors such as data sensitivity, operational impact, automation level, customer exposure, regulatory obligations, system integration, or governance review outcomes. Requirements assigned as 'Conditional' will be assessed on a case-by-case basis.
- **Required**: The control must be implemented and maintained for the specified governance tier prior to production or operational use.
- **N/A**: This control is designated for use cases assigned to Tier 4, where not all controls will apply as Tier 4 use cases are not permitted to move forward.

Escalation Process for High Governance Tier

Use cases assigned to Tier 4 will require VP review of the use case context. The controls labeled 'Required' for Tier 4 are those deemed necessary to implement to provide the VP with the necessary context to review the AI system.

Control ID	Control	Tier 1	Tier 2	Tier 3	Tier 4
GOV-01	Business owner identified	Required	Required	Required	Required
GOV-02	Use case registration	Required	Required	Required	Required
GOV-03	Technical Owner Identified	Conditional	Required	Required	Required
GOV-04	AI Impact Assessment	Required	Required	Required	Required

DATA-01	Data classification documented	Required	Required	Required	Required
DATA-02	Data sources documented	Not required	Required	Required	Required
DATA-03	Data flow documented	Not required	Conditional	Required	VP Review
HUM-01	Human override mechanism	Not required	Conditional	Required	VP Review
HUM-02	Human review	Required	Required	Required	Required
TEST-01	Consistency	Not required	Required	Required	VP Review
TEST-02	Bias testing	Not required	Required	Required	VP Review
TEST-03	Explainability validation	Not required	Conditional	Required	VP Review
MON-01	Ongoing monitoring	Required	Required	Required	VP Review
MON-02	Drift detection	Not required	Conditional	Required	VP Review
MON-03	Output validation	Conditional	Required	Required	VP Review
LIFE-01	Risk assessment	Conditional	Required	Required	Required
LIFE-02	Re-tiering review	Required	Required	Required	VP Review
LIFE-03	Incident reporting	Not required	Required	Required	VP Review
LIFE-04	Documentation upkeep	Required	Required	Required	Required
LIFE-05	Decommission-ing Process	Required	Required	Required	VP Review
OPS-01	Error handling	Conditional	Required	Required	VP Review

Control Ownership Assignments

The following matrix outlines the stakeholder ownership responsibilities for each control seen above. The roles are either the control Submission Owner, or the control Reviewing/Supporting stakeholder:

- **Submission Owner:** The primary stakeholder responsible for properly completing, maintaining and submitting the control, documentation, evidence, assessment, or governance requirements for review as part of the AI governance process.

- **Reviewing/Supporting Stakeholder:** Stakeholder groups responsible for reviewing, validating, approving, advising on, implementing, monitoring, or supporting the control based on

their applicable governance, operational, security, privacy, legal, compliance, or technical responsibilities.

Control ID	Control	Submission Owner	Reviewing/Approving Stakeholder
GOV-01	Business owner identified	Business Owner	AI Governance
GOV-02	Use case registration	Business Owner	AI Governance
GOV-03	Technical Owner Identified	Technical Owner	AI Governance, Enterprise Architecture
GOV-04	AI Impact Assessment	Business Owner	AI Governance, Privacy, Cybersecurity
DATA-01	Data classification documented	Business Owner	Data Governance
DATA-02	Data sources documented	Technical Owner	Data Governance, Enterprise Architecture
DATA-03	Data flow documented	Technical Owner	Data Governance, Enterprise Architecture
HUM-01	Human override mechanism	Technical Owner	Enterprise Architecture, AI Governance
HUM-02	Human review	Business Owner	AI Governance
TEST-01	Consistency	Technical Owner	Enterprise Architecture, AI Governance
TEST-02	Bias testing	Technical Owner	Legal, Business Ethics & Compliance, Privacy, AI Governance, EEO
TEST-03	Explainability validation	Technical Owner	AI Governance
MON-01	Ongoing monitoring	Technical Owner	Enterprise Architecture
MON-02	Drift detection	Technical Owner	Enterprise Architecture
MON-03	Output validation	Business Owner	Enterprise Architecture
LIFE-01	Risk assessment	Business Owner	Enterprise Architecture, AI Governance, Cybersecurity, Privacy, Business Ethics & Compliance, EEO, Legal
LIFE-02	Re-tiering review	Business Owner	AI Governance
LIFE-03	Incident reporting	Business Owner	AI Governance, Enterprise Architecture, Cybersecurity, Privacy
LIFE-04	Documentation upkeep	Technical Owner	AI Governance, Enterprise Architecture

LIFE-05	Decommission-ing Process	Technical Owner	Enterprise Architecture

Controls by Category

Governance

Evidence required

Tier 1:

- Approved use case registration
- Business owner identified
- Technical owner identified (if applicable)

Tier 2:

- Same as tier 1 requirements

Tier 3:

- Same as Tier 1 requirements
- Formal AI Risk and Impact assessment documented and reviewed
- Formal governance approval documentation
- Senior business and governance approval required in accordance with the Human Oversight & Escalation Guidelines

Tier 4:

- Executive review required

GOV-01 - Business owner identified: All tiers

Definition: A designated individual accountable for the AI system's business purpose, governance compliance, and operational outcomes.

Source: NIST GOVERN

GOV-02 - Use case registration: All tiers

Definition: The process of documenting and submitting an AI system or AI-enabled use case into the organization's AI governance process prior to deployment or operational use. Registration captures key information needed to assess risk, assign governance requirements, and determine appropriate controls and oversight obligations.

Source: NIST GOVERN

GOV-03 - Technical owner identified: All tiers

Definition: A designated technical resource responsible for implementation, maintenance, monitoring, and technical issue resolution.

Source: NIST GOVERN

GOV-04 - Formal AI impact assessment: Tier 3

Definition: A documented assessment evaluating operational, legal, privacy, security, ethical, and reputational risks associated with high-impact AI systems.

All tier 3 use cases require completion and approval of a formal AI Impact Assessment prior to production deployment.

Source: NIST GOVERN

Data

Evidence required

Tier 1:

- High level documentation of data sensitivity submitted.
- Primary data sources used by the AI system identified.

Tier 2:

- Data classification formally documented & approved for all data sources.
- Internal, external, and third-party data sources documented.
- Data flow documented for specific use case reviewed and approved (if applicable).

Tier 3:

- Data classification formally documented & approved for all data sources.

- Formal documentation and approval for all data sources, repositories, retrieval mechanisms, training datasets, and output repositories.
- Formal data flow documentation submitted and approved.

Tier 4:

- Executive review required

DATA-01 - Data classification documented: All tiers

Definition: Identification and documentation of the sensitivity level and handling requirements for data used, processed, stored, or generated by the AI system in accordance with enterprise data governance standards.

Tier guidance:

- Tier 1: Basic awareness of data sensitivity is required for use case intake and governance review.
- Tier 2: Data classification documentation required for all connected or processed business data.
- Tier 3: Formal documented classification and approval required for all input, output, training, retrieved, or stored data sources.
- Tier 4: Executive review required

Source: NIST MANAGE 1, 2

DATA-02 - Data sources documented: All tiers

Definition: Documentation of the origin, ownership, and intended use of data sources connected to or used by the AI system.

Tier guidance:

- Tier 1: High-level documentation of primary data sources is sufficient.
- Tier 2: All material internal, external, and third-party data sources must be documented.
- Tier 3: Formal documentation required for all production data sources, integrations, retrieval mechanisms, training datasets, and generated output repositories.
- Tier 4: Executive review required

Source: NIST MANAGE 2

DATA-03 - Formal data flow documentation: Tier 2; Tier 3

Definition: Documentation describing how data flows through the AI system, including data origin, movement, transformation, storage, usage, and output generation processes.

Tier guidance:

- Tier 2: Required where sensitive, regulated, integrated, customer-facing, or multi-source data is involved.
- Tier 3: Formal data flow documentation required, including upstream and downstream system dependencies where applicable.
- Tier 4: Executive review required

Source: NIST MANAGE 2

Human oversight

Evidence required:

Tier 1:

- High level description of review process of outputs.

Tier 2:

- Documentation outlining human review responsibilities within the use case reviewed & approved.
- Human override and operational suspension mechanisms formally documented, tested, and approved.

Tier 3:

- Formal human oversight procedures have been documented and approved.
- Human override and operational suspension mechanisms formally documented, tested, and approved.
- Formal documentation and approval of escalation mechanisms, as well as authority and response procedures.

Tier 4:

- Executive review required

HUM-01 - Human override mechanism: Tier 2; Tier 3

Definition: A capability allowing authorized individuals to intervene in, override, pause, disable, or prevent AI-generated outputs, actions, or automated processes when necessary.

Tier guidance:

- Tier 2: Required for AI systems involving workflow automation, system integration, or consequential operational support.
- Tier 3: Formal override and escalation mechanisms required, including clearly defined authority and response procedures, as well as operational suspension capabilities documented and in place.
- Tier 4: Executive review required

Source: NIST MANAGE 1, 4

HUM-02 - Human review: All tiers

Definition: AI-generated outputs must be subject to appropriate human review and oversight proportional to the system's risk, intended use, and potential impact.

Tier guidance:

- Tier 1: Manual or ad hoc review may be sufficient for low-risk or assistive use cases.
- Tier 2: Human review required prior to consequential operational, business, customer-facing, or decision-support use.
- Tier 3: Formalized human oversight procedures required, including documented review responsibilities, escalation paths, and accountability mechanisms.
- Tier 4: Executive review required

Source: NIST MANAGE 1, 4

Testing

Evidence required:

Tier 1:

- Any identified issues or limitations have been documented and addressed, where appropriate.
- Formal testing processes outlined if applicable.

Tier 2:

- Required testing completed prior to production, with the results/process documented and reviewed.
- Identified issues or limitations documented and addressed where appropriate.
- Ongoing testing or periodic reassessment procedures and requirements documented and approved if applicable.

Tier 3:

- Formal testing activities have been completed or documented.
- Testing results, limitations, or identified risks have been reviewed and approved.
- Ongoing testing or periodic reassessment procedures and requirements documented and approved if applicable.

Tier 4:

- Executive review required

TEST-01 - Consistency testing: Tier 2; Tier 3

Definition: Testing performed to evaluate whether the AI system consistently produces accurate, stable, and appropriate outputs aligned with its intended purpose and operational requirements.

Testing may include evaluation of:

- output consistency
- accuracy
- stability
- failure handling
- operational performance
- alignment with business outcomes

Tier guidance:

- Tier 2: Consistency testing required prior to production or operational use.
- Tier 3: Formalized and documented consistency testing required, including representative use cases, edge cases, and failure scenario testing where applicable.
- Tier 4: Executive review required

Source: NIST MANAGE 1

TEST-02 - Bias testing: Tier 2; Tier 3

Definition: Testing performed to identify, assess, and mitigate potential unfair, discriminatory, or unintended biased outcomes generated by the AI system.

Tier guidance:

- Tier 2: Required for customer-facing, employee-impacting, decision-support, or other consequential use cases.
- Tier 3: Formalized and documented bias testing required prior to deployment and periodically thereafter, as applicable.
- Tier 4: Executive review required

Source: NIST MANAGE 1

TEST-03 - Explainability validation: Tier 2; Tier 3

Definition: Evaluation of whether AI system outputs, recommendations, or behaviors can be reasonably understood, interpreted, and explained by appropriate stakeholders.

Where applicable, validation should also confirm that appropriate user-facing notices, disclosures, or transparency requirements related to AI system usage have been implemented for affected customers, employees, or other stakeholders.

Tier guidance:

- Tier 2: Conditional based on system complexity, customer impact, operational significance, or decision influence.

- Tier 3: Required, including documented rationale for model transparency, interpretability approach, or human review controls where direct explainability is limited.
- Tier 4: Executive review required

Source: NIST MANAGE 1

Monitoring

Evidence required

Tier 1:

- Behavioral issues, unintended outputs, or potential misuse identified through testing, monitoring, or human oversight are documented, assessed, and addressed.

Tier 2:

- Documented monitoring procedures and assigned ownership.
- Evidence of implemented drift detection or equivalent performance monitoring processes, where applicable.
- Monitoring review cadence and escalation paths documented.
- Monitoring records and identified remediation activities retained for governance review

Tier 3:

- Formal monitoring procedures documented, approved, and periodically reviewed.
- Evidence of approved drift detection, performance monitoring, or equivalent oversight mechanisms maintained.
- Monitoring ownership, escalation procedures, review cadences, and response thresholds formally defined.
- Evidence of ongoing review for security concerns, misuse, harmful outputs, model degradation, or performance changes maintained.

Tier 4:

- Executive review required

MON-01 - Ongoing monitoring: All tiers

Definition: Processes established to continuously or periodically monitor AI system performance, usage, consistency, operational behavior, and compliance throughout the system lifecycle.

Tier guidance:

- Tier 1: Monitoring performed upon changes to use case involving expanded/additional data access, or an increase to the autonomy or decision-making capability of the AI system.
- Tier 2: Monitoring performed at least quarterly.
- Tier 3: Monitoring performed at least monthly and reviewed by designated stakeholders.
- Tier 4: Executive review required.

Source: NIST MANAGE 3

MON-02 - Drift detection: Tier 2; Tier 3

Definition: Monitoring processes used to identify degradation in AI system performance, unexpected behavioral changes, reduced accuracy, or shifts in input/output patterns over time.

Tier guidance:

- Tier 2: Quarterly where applicable; conditional based on operational integration, automation level, model complexity, customer impact, or data sensitivity.
- Tier 3: Drift detection performed at least monthly.
- Tier 4: Executive review required.

Source: NIST MANAGE 3

MON-03 - Output validation: All tiers

Definition: Validation processes used to assess whether AI-generated outputs are accurate, reliable, appropriate, and aligned with the system's intended purpose and business requirements.

Tier guidance:

- Tier 1: Manual or ad-hoc validation sufficient for low risk use cases if required.
- Tier 2: Reviews to be conducted quarterly.

- Tier 3: Reviews to be conducted at least monthly.
- Tier 4: Executive review required.

Source: NIST MANAGE 3

Lifecycle governance

Evidence required

Tier 1:

- Simplified lifecycle governance activities may be sufficient for low-risk or experimental use cases, including basic documentation of the intended use, ownership, applicable risks, and any required safeguards or oversight measures proportional to the system's risk profile.

Tier 2 & Tier 3:

- Documented risk assessment reviewed and approved.
- Procedure documented and approved for re-tiering/reassessment review upon meaningful changes to the AI system.

Tier 4:

- Executive review required.

LIFE-01 - Risk assessment: All tiers

Definition: Formal evaluation and documentation of operational, legal, compliance, privacy, security, ethical, reputational, and business risks associated with the AI system beyond initial risk tier classification activities.

Tier guidance:

- Tier 1: Risks, incidents, or changes pertinent to the nature of the AI system can be identified and escalated when necessary.
- Tier 2: Annually or upon change in use case.
- Tier 3: Quarterly or upon substantive change in the use case.

- Tier 4: Executive review required.

Risk assessments should be updated when substantive changes occur to the AI system, underlying model, connected data sources, or intended use case.

Source: NIST MANAGE 1,4

LIFE-02 - Re-tiering review: All tiers

Definition: Review performed to determine whether an AI system's assigned governance tier remains appropriate following material changes to the system, data, integrations, operational scope, or intended use.

Tier guidance:

- All AI use cases, regardless of assigned tier, will need to be submitted for re-tiering at least annually. Additionally, re-tiering must be initiated upon any substantive change in scope, data, integration, automation, or audience.

Source: NIST MANAGE 2,4

LIFE-03 - Incident reporting: All tiers

Definition: Processes established to identify, document, escalate, and respond to AI-related incidents, failures, harmful outputs, policy violations, security concerns, or operational issues.

Tier guidance:

- Tier 1: Reporting of significant incidents or policy violations is recommended.
- Tier 2: Formal documented incident management and escalation procedures required, including governance notification and remediation tracking.
- Tier 3: Formal documented incident management and escalation procedures required, including governance notification and remediation tracking.
- Tier 4: Executive review required.

Source: NIST MANAGE 4.3

LIFE-04 - Documentation upkeep: All tiers

Definition: Processes established to ensure governance documentation, approvals, assessments, inventories, and supporting evidence remain accurate, current, and appropriately maintained throughout the AI system lifecycle.

Tier guidance:

- All tiers: Reviewed annually or upon substantive change in use case.

Source: NIST MANAGE 2; GOVERN 1.4.

LIFE-05 - Decommissioning process: All tiers

Definition: Processes established to retire, disable, remove, or discontinue AI systems in a controlled manner while addressing operational, security, data governance, compliance, and documentation requirements.

Decommissioning reviews should confirm that:

- operational dependencies have been addressed
- monitoring activities have been terminated appropriately
- and residual risks associated with retirement have been evaluated

Source: NIST MANAGE 2.4.

Operations

OPS-01 - Evidence required

Tier 1:

- Users express understanding of error handling procedures and when those might be necessary.

Tier 2:

- Formal error handling and remediation procedures have been documented and approved.
- Roles and responsibilities for issue identification and resolution are defined and approved.

Tier 3:

- Formal error handling and remediation procedures have been documented and approved.
- Roles and responsibilities for issue identification and resolution are defined and approved.
- Escalation process to necessary stakeholders upon operational issues documented and approved.

Tier 4:

- Executive review required.

Error handling: All tiers

Definition: Processes and controls established to identify, manage, respond to, and remediate AI system errors, failures, inaccurate outputs, unexpected behavior, or operational issues.

Tier guidance:

- Tier 1: Informal or manual error handling processes may be sufficient for low-risk or experimental use cases.
- Tier 2: Documented error handling procedures required for operational or production AI systems.
- Tier 3: Formalized and documented error handling and remediation processes required, including escalation procedures, issue tracking, and defined response ownership.
- Tier 4: Executive review required.

Source: NIST MANAGE 1,4

NOTICE TO CUSTOMERS, OTHERS

Attachment 4

CEI-211 CI Protection of Personally Identifiable Information (PII)

CEI-407 Data Classification

CEI-408 Protection of Critical Energy Infrastructure Information

870-1 CI Records Management

conEdison, inc.

Corporate Instruction

SUBJECT

CEI-211 CI Protection of Personally Identifiable Information (PII)

1.0 PURPOSE -- To provide instruction and assign responsibilities for protecting personally identifiable information (PII) and to provide guidance for reporting and responding to a potential incident when PII is accessed or acquired without authorization.

2.0 APPLICATION -- This procedure applies to Consolidated Edison, Inc. (CEI) and its subsidiaries that use or maintain PII in any form, including electronic or paper. Such PII may relate to customers, employees, retirees, contractors, vendors, or other individuals and may be handled by CEI, its subsidiaries, and its affiliates.

3.0 DEFINITIONS --

3.1 Electronic and Paper PII – PII in electronic form includes information that is stored, distributed, reported, or transmitted via computerized magnetic tapes, computer disks, or other electronic media or means of transmission, whereas PII handled in a paper form includes, among other examples, personnel files or printed customer records.

3.2 Restricted Information – Any PII in CEI's possession which is considered "Restricted" per CEI-407 Data Classification and should be handled according to that policy. Additionally, the Standards of Business Conduct, available online at https://www.conedison.com/-/media/files/conedison/standards-of-business-conduct.pdf, discusses the need to protect this information. (Reference CEI Corporate Policy Statement CEI-010 Standards of Business Conduct).

3.3 PII – Any information that can be used to identify any individual (for example, name, address, date of birth or other personal mark) in combination with any one of the following data elements. The data elements include:

a. Social Security number or any derivation thereof, such as the last four digits of a Social Security number.

b. Government issued identification, including, for example, driver's license, non-driver's identification information, such as New York City Identity Card ("IDNYC"), Individual Taxpayer Identification Numbers ("ITIN"), military identification information, and passports.

c. Individual financial account number or individual financial account number and personal identification number ("PIN") or password, including debit or credit card information.

d. Information related to an individual's medical and psychiatric history, mental or physical condition, human immunodeficiency virus (HIV) or psychiatric status and any Personal Health Information (PHI) as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) shared under CEI's group health plan.

e. User name or e-mail address in combination with a password or security question and answers, such as mother's maiden name, which grants access to an account or system containing PII.

f. Drug and alcohol test results.

g. Biometric and genetic information, such as fingerprints, voice prints and signatures.

4.0 GENERAL PROVISIONS --

4.1 Protection and Handing of PII – PII should be treated with care and must be protected so that only authorized individuals have access to the information. Each organization with business applications containing PII shall implement security administration procedures, including at least an initial approval for access and an annual process for reapproving access, for these applications. Revoking access when it is no longer required may be an automated or manual process. The daily HR Transaction Workbook contains a comprehensive list of all employee terminations and transfers, and should be used by Consolidated Edison Company of New York, Inc. (CECONY) and Orange and Rockland Utilities, Inc. (O&R) application security administrators to identify employees who no longer require access to applications containing PII. That access should be removed immediately. All movement of both physical and electronic PII will use appropriate controls (such as encryption) to prevent inadvertent disclosure. For example, PII should always be protected, secured, and never left unattended because loss of this information may allow an individual to be identified.

4.2 Minimizing PII – Employees should use care in handling, maintaining, and storing any PII. Employees should minimize the need to collect PII and maintain what is collected in accordance with established procedures or guidelines, limiting the number of employees with access to such information. Any records and systems containing PII should be reviewed regularly so that the data is

retained and preserved in accordance with 870- 1 CI Records Management and other applicable policies. If there is no retention policy and the information is no longer needed, it should be properly discarded or destroyed.

4.3 Handling a Breach –

a. Actual and suspected incidents involving potential unauthorized access to or acquisition of PII, regardless of apparent significance/severity, are to be communicated to the PII Incident Response Team (which consists of representatives from CECONY's Corporate Security, Information Technology, and Law). To notify the PII Incident Response Team, employees may:

- Call 1-212-PRIVACY or 1-212-774-8229 or send an e-mail to dl – PII Incident Response Team.
- Contact their supervisor who should call or e-mail the PII Incident Response Team to communicate the incident.

b. The PII Incident Response Team will review and address reports of incidents related to the unauthorized access or acquisition of any type of PII, whether intentional or inadvertent, in accordance with the PII Incident Response Plan. The PII Incident Response Team will determine what actions, if any, should be performed and direct the appropriate response under the Personal Information Incident Response Plan. The Personal Information Incident Response Plan describes the actions that should be taken in the event of an incident.

5.0 ADVICE AND COUNSEL -- CEI's Senior Vice President and General Counsel, CECONY's Vice President of Customer Operations, and CECONY's Senior Vice President and Chief Information Officer, will provide advice and counsel on this Instruction.

6.0 POLICY OWNER -- The Director and Chief Privacy Officer.

7.0 REVIEW CYCLE -- This Corporate Instruction is reviewed every two years.

8.0 SUMMARY OF CHANGES –

conEdison, inc.

Corporate Instruction

SUBJECT

CEI-211 CI Protection of Personally Identifiable Information (PII)

APPROVAL DATE	SUMMARY OF CHANGES
January 18, 2025	• Section 3.2 – Updated 'Restricted Information' Reassigned data classification for PII as Restricted, from Confidential; added date of birth to PII definition. • Section 4.1 – Updated 'Protection and Handling of PII' • Section 4.2 – Updated 'Minimizing PII' • Section 4.3 - Updated 'Privacy Team' to 'PII Incident Response Team'. • Section 5.0 – Updated 'SVP Customer Operations' to 'VP Customer Operations and CECONY's VP IT to 'SVP and Chief Information Officer'. • Section 6.0 – Updated policy owner to Director and Chief Privacy Officer.
March 10, 2023	• Section 4.1 – Removed 'Con Edison Clean Energy Businesses, Inc. (CEB) Human Resources will notify CEB IT – Infrastructure via a "Termination Form" or "Employee Change Form" of any required changes to authorizations due to employee terminations or transfers.' Due to the sale of CEB, this is no longer applicable.
December 18, 2021	• Section 3.3 b – Added "military identification information." • Section 3.3 c – Added "Personal identification number ("PIN") or password, including debit or credit card information." • Section 5.0 – Removed Chief Information Officer and added Engineering and Operations.

conEdison, inc.

Corporate Policy Statement

SUBJECT

CEI-407 Data Classification

1.0 PURPOSE -- To protect the restricted and confidential information of the Company or in the Company's possession by establishing a data classification policy.

2.0 APPLICATION – This Policy applies to Consolidated Edison, Inc. (CEI) and its subsidiaries, including Consolidated Edison Company of New York, Inc. (CECONY); Orange and Rockland Utilities, Inc. (O&R); Con Edison Transmission, Inc. (CET); and their affiliates and third parties working on behalf of the CEI (collectively, the Company) that maintain, use, or process data in any format. Data classification policy defined herein applies to all written, recorded, electronic, or graphic data or information (data) that is created, collected, stored, or processed by the Company in the course of its business. This Policy is applicable to data created or reviewed after the effective date of this Policy.

3.0 GENERAL PROVISIONS --

3.1 DEFINITIONS –

Data – All written, recorded, or graphic information that is created, collected, stored, or processed by the Company in the course of its business.

Data Creator – The individual who creates the data to be classified.

Data Owner – The person with oversight and responsibility for the data based on Company-assigned role. The Data Owner determines how the data is to be used and shared. Typically, the Data Owner is responsible for the process which uses the data in question. Data Owners include the business owners of information systems and the sponsors of content repositories, such as server shares and directories, SharePoint sites, Exchange folders, and personal computer files. Data Owners determine administrative controls required to protect the data in information systems and content repositories.

Data User – Anyone with access to the data or systems which store the data.

Document – Memoranda, reports, drawings, emails, or files created using common formats including PDF, Word, Excel, PowerPoint, or similar types regardless of media in which the document is stored (e.g., paper, electronic, microfiche).

3.2 DATA CLASSIFICATION –

Classifying data is the process of categorizing data assets based on the sensitivity of the data processed. When assessing classification, personnel should consider if laws and/or regulations apply to the data, and any risk to the organization and/or individuals if the

data is inadvertently disclosed or becomes public. Those assets are then securely managed based on the classification.

Data assets shall be classified using one of the following categories:

Classification	Examples	Impact of Exposure
Public Data and/or documents that are non-sensitive in nature, approved for general or public use.	• Press releases • Marketing materials • Customer service offerings • Company job postings • General Information (e.g., lunch invitation)	None
Internal Data and/or documents handled on a day-to-day basis, belonging to and intended for general availability within the Company, and not intended for public disclosure.	• Employee newsletters • Corporate instructions, personnel policies, organization procedures • Employee work schedules, directory information, contact lists, organizational charts • Vendor business contact information (Address, Email, Phone, etc.) • Business-related communications and documents shared with external business partners for business purposes	Limited harm to the Company if disclosed outside the Company.
Confidential Data and/or documents of a proprietary or sensitive nature that are intended for internal use only and access to which should be limited to a "need to know" basis, indicating that loss or unauthorized disclosure of this information would impact the operation, finances, reputation, and/or legal or contractual obligations of the Company.	• Personal Information (PI) of an individual including name, address, customer electric, gas or steam usage information, account number • Sensitive information about an individual such as race, religion, ethnicity, political affiliation, sexual orientation, gender preferences or identification. • Company nonpublic financial information or strategy documents • Customer proposals, quotes, and contracts • Corporate Security investigation information, unless marked as attorney client privilege • Financial and operational data • Select research and development project information, files, and documents • Business and marketing plans • Salary planning and information • State and Federal regulatory filings (prior to filing)	Material harm to the Company, our customers, vendors, business partners, and/or shareholders resulting in legal or financial liability, adverse competitive impact, financial loss, and/or reputational harm if disclosed outside the Company.
Restricted Data and/or documents of a highly sensitive information nature that is protected by law or contractual obligations, or information that could	• Personally Identifiable Information (PII), as defined in CEI CI-211 • Personal Health Information, including electronic (PHI/ePHI) • Customer, employee, and Company financial data (credit/debit card numbers, bank, or other financial accounts)	Significant or severe harm to the Company, our customers, vendors, business partners, and/or shareholders resulting in legal or financial liability, adverse competitive impact,

cause serious impact to the Company or individuals if disclosed to unauthorized persons or entities.	• Usernames in combination with passcodes, PINs, and passwords • Detailed financial data about certain company operations and profitability (e.g., wholesale energy contracts) • Critical Energy Infrastructure Information (CEII) as defined in CEI-408 • NERC CIP and Bulk Electric System Cyber System Information (BESCSI) as defined in CEI-408 • Information marked as Attorney-Client Privileged • Potential mergers and acquisition information • Corporate network security information, including IT network configuration information (e.g., network diagrams) • Material non public information as defined in CEI-406	financial loss, and/or reputational harm if disclosed outside the Company.

3.3 DATA HANDLING –

Data handled via email should be assigned the appropriate Outlook Sensitivity label based on the assessed data classification.

Data handled via documents should include the appropriate labeling based on the assessed data classification.

Data handled via hard copy should be stored with appropriate securing mechanisms based on the assessed data classification.

Restricted or Confidential data may be shared by CECONY and O&R with contractors and vendors qualified though Supply Chain in accordance with corporate policy and who meet the specifications in Corporate Instruction 320-14, Acquisition of Materials, Supplies, or Services as applicable. CET should ensure vendor compliance with the requirements of this Corporate Policy. Restricted or Confidential data may be shared for certain business purposes with individuals, companies, associations, or government agencies. Company employees providing information to government agencies shall follow any requirements of such agency for the protection from disclosure of Restricted or Confidential data. A non-disclosure agreement (NDA) or applicable legal confidentiality requirement between any CEI entity sharing the information and the vendor, contractor, individual, company, or association is required absent exigent circumstances. NDAs or applicable legal confidentiality requirements with government agencies are recommended, subject to agency policies.

3.4 DATA SECURITY –

Data created as part of Company employment or using company resources is considered Company property. This data shall be shared using appropriate judgment.

Data must be protected in accordance with CECONY's standard security requirements, which are identified in the Con Edison Information Security Policy, and pursuant to the controls below:

Limit access to only those who need to use Confidential data to perform their work.

Do not share passwords enabling data access.

Store hard-copy documents and physical media containing Confidential data (e.g., CDs, USB drives) in locked or secured offices, desks, file cabinets, or other secured locations.

At all times, physically secure documents or electronic devices containing Confidential data during transport.

Encrypt Confidential data during transmission outside of Con Edison's computer network (including via e-mail) or when saving on removable storage media.

Ship physical media or documents containing Confidential data using Company preferred shipping carriers and methods. Materials should be encrypted and/or sealed securely inside shipping envelopes/boxes.

The Data Owner's organization may specify training requirements and any additional requirements for access to and handling of certain Confidential data.

When disposing of Confidential data, documents and media must be destroyed completely to preclude recognition or reconstruction of the information contained in or on the material.

3.5 DECLASSIFICATION OF DATA –

Data can be declassified if it no longer meets the standards and criteria for classification. The authority to declassify information resides with the Data Owner, who is encouraged to consult with the Advice and Counsel contacts for this policy.

4.0 RESPONSIBILITIES --

Data Creators and Data Owners are responsible for classifying data with the appropriate category and handling protocols as described in paragraphs 3.2 and 3.3 above.

Agreements with third parties must contain appropriate confidentiality and security provisions based on the sensitivity of the data. In consultation with the Law Department,

Data Owners review confidentiality and security provisions in agreements with external entities to address data classification requirements.

If data is suspected to be lost or accessed without authorization, the PII Incident Response Team must be contacted immediately.

The PII Incident Response Team can be contacted at dl – PII Incident Response Team.

The Privacy Compliance team can be contacted at PrivacyCompliance@coned.com or 212-Privacy / (212)774-8229.

For more information on Data Privacy you can access, Privacy Compliance (sharepoint.com)

5.0 REFERENCES –

CEI CI-211 CI Protection of Personally Identifiable Information (PII) (sharepoint.com)

CEI-408 Protection of Critical Energy Infrastructure Information (sharepoint.com)

CEI-406 Insider Trading (sharepoint.com)

6.0 ADVICE AND COUNSEL -- CECONY's Vice President of IT Engineering, Operations, and Cybersecurity, the Director of Corporate Security and the Vice President of Energy and Environmental Law will provide advice on this Policy.

7.0 POLICY OWNER – Director Privacy Compliance, Business Ethics & Compliance

8.0 REVIEW CYCLE -- This Corporate Policy Statement is reviewed every five years.

9.0 SUMMARY OF CHANGES --

APPROVAL DATE	SUMMARY OF CHANGES
10/14/25	• Removed footnote 1 and replaced with hyperlink, 'Con Edison Information Security Policy'.
9/17/2023	• Updated policy to include new required data classifications. • Replaced two categories (General and Confidential) with four, including a new chart of definitions with examples of each. • Updated Data Handling instructions to encourage use of Outlook labels and document templates.

	• Edited to remove procedural language, to be included in a future accompanying handling procedure with release of automated controls.

conEdison, inc

Corporate Policy Statement

SUBJECT

PROTECTION OF CRITICAL ENERGY INFRASTRUCTURE INFORMATION

1.0 **PURPOSE** -- To provide Consolidated Edison, Inc. (CEI) and its subsidiaries with responsibilities for protecting Critical Energy Infrastructure Information (CEII), and to provide guidance for labeling and controlling access to materials that include CEII.

2.0 **APPLICATION** -- This Corporate Policy Statement applies to CEI, Consolidated Edison Company of New York, Inc. (CECONY), Orange and Rockland Utilities, Inc. (O&R), Con Edison Transmission, Inc. (CET), and their affiliates (collectively, the Company or Corporate), that maintain or use CEII in any format, including electronic or printed documents.

3.0 **GENERAL PROVISIONS** -- The CEII Corporate Policy Statement (CEII Policy) is to provide greater protection of the Company's systems and assets.

3.1 **Definitions –**

a. Critical Energy Infrastructure is a system or asset, whether physical, cyber or virtual, the disruption, incapacity, or destruction of which would negatively affect national, state, or local physical security, economic security, public health or safety, or any combination thereof.

b. CEII is any specific engineering, vulnerability, or detailed design information about proposed or existing critical energy infrastructure (production, generation, transportation, transmission, or distribution of energy, including electric, gas or steam) that:

c. Could be useful to a person/entity in planning an attack on critical energy infrastructure; and

d. Provides information beyond general location of critical energy infrastructure.

e. Bulk Electric System Cyber System Information (BCSI) is a subcategory of CEII. BCSI will be handled and marked based on policies in the CEI departments creating, handling, and storing BCSI. BCSI does not need to be marked as CEII.

3.2 All potential CEII materials must be evaluated, using the general criteria of Section 3.1, above, on a case-by-case basis. The following examples are for guidance only.

a. Materials **typically** considered as containing CEII include transmission short-circuit, power-flow, and dynamic models of system maps and

diagrams, pipeline studies, certain next worst contingency studies on a case-by-case basis, System Operations Contingency Plans, critical asset lists, assessments of vulnerabilities, restoration plans, and high tension operating diagrams, including for CECONY, its 900 diagram, or, for O&R, its bulk power system diagram.

b. Materials typically not considered as containing CEII include ten-year load forecasts, individual area or project studies, and construction documents that do not contain the location of critically important facilities.

4.0 PROCEDURES --

4.1 CEII Obligation – Any Department or Senior VP Organization that handles CEII is required to develop a procedure for implementing the CEII Policy within 90 days of its effective date. This procedure shall establish a process by which the Department or Organization drafts, creates or revises documentation, and how it will be evaluated, marked, and/ or handled as CEII.

4.2 Evaluating and Marking CEII –

a. The drafter, creator, or revisor of materials is responsible evaluating whether the content is CEII and to mark it appropriately, in accordance with their Department's procedures for implementing the CEII Policy.

b. Every employee has a continuing obligation to evaluate whether materials contain CEII. Employees who believe existing material should be marked as CEII must notify the Department that originally created the document, as well as Energy and Environmental Law if necessary, that the document should be evaluated as potentially CEII in accordance with the Department's procedures for implementing the CEII Policy.

c. All materials determined to be CEII must be marked as "RESTRICTED – CRITICAL ENERGY INFRASTRUCTURE INFORMATION." Additional information and details on marking documents are available in Corporate Policy Statement CEI-407, Data Classification (CEI-407).

4.3 Handling CEII –

a. See CEI-407 Sections 3.4 and 4.2.

b. Departments that create, store, access, or share CEII should perform a periodic access review of the employees granted access to CEII.

4.4 Sharing CEII –

a. The Company may share CEII with contractors and vendors. For CECONY and O&R, those contractors and vendors must be qualified through Supply Chain in accordance with corporate policy and meet the specifications in Corporate Instruction 320-14, Acquisition of Materials, Supplies or Services (CI-320-14) when applicable. CET should ensure vendor compliance with the requirements of this Corporate Policy Statement, including CEII marking and handling requirements.

b. The Company may, for certain business purposes, share CEII with individuals, companies, associations or government agencies. This includes the information that Con Edison System and Transmission Operations (S&TO) and O&R Transmission and Substation Engineering regularly provide to the New York Independent System Operator (NYISO); PJM Interconnection (PJM); ISO-New England and other New York Control Area (NYCA)/PJM Transmission Owners to maintain reliability and perform required studies. Company employees providing information to government agencies shall follow any requirements of such agency for the protection from disclosure of Company CEII.

c. A non-disclosure agreement (NDA) or applicable legal confidentiality requirement between any CEI entity sharing the information and the vendor, contractor, individual, company, or association is required absent exigent circumstances. NDAs or applicable legal confidentiality requirements with government agencies are recommended, subject to agency policies.

5.0 RESPONSIBILITIES --

a. Energy and Environmental Law will provide legal advice and counsel on federal and state laws and regulations related to CEII and the development of procedures for implementing the CEII Policy.

b. Enterprise Technology and Security will provide advice on technology protection for CEII data, communication, and computer facilities.

c. Each operating group will provide advice on its own facilities.

d. The Insider Threat Team is responsible for investigating reported incidents involving suspected or confirmed violations of this policy, including unauthorized access, handling, or disclosure of Critical Energy

Infrastructure Information (CEII). As noted in CI 590-3, Insider Threat Program (InTP), employees must report potential Insider Threats to their supervisor, and/or the Ethics Helpline or by a Security Incident Report at the following link https://coned.ethicspointvp.com/custom/coned/forms/security/form_data.asp

6.0 REFERENCES --

6.1 FERC: FAST Act, Pub. L. No. 114-94, § 61,003, 129 Stat. 1312, 1773-1779 (2015) (codified as 16 U.S.C. § 824o-1 (2018)) and FERC's regulations at 18 C.F.R. § 388.113 (2020).

6.2 New York: New York Public Officers Law ("POL") §87.2(b) & (f), POL §89.5(a)(1)(1-a) and the Commission's implementing regulations at 16 NYCRR §6-1.3.

6.3 New Jersey: N.J.S.A App A: 9-68, 9-74a and the Board's implementing regulations at N.J.A.C. 14:3-6.7.

6.4 CI 590-3 Insider Threat Program (InTP)

7.0 ADVICE AND COUNSEL -- CECONY's Chief Security Officer and CECONY's Vice President of Energy and Environmental Law will provide advice and counsel on this Corporate Policy Statement.

8.0 POLICY OWNER -- CECONY's Chief Security Officer.

9.0 REVIEW CYCLE -- This Corporate Policy Statement is reviewed every five years.

10.0 SUMMARY OF CHANGES --

Approval Date	Summary of Changes
9/5/26	Section 4.3, 5.0(b), 6.4 , 7.0, and 8.0 Updated. Updated Organization name from Information Technology to Enterprise Technology and Security.
3/15/23	Sections 2.0 and 4.4 – Removed references to CEB; Sections 4.2b., 5.0a., 7.0 – Changed 'Regulatory Services' to 'Energy and Environmental Law'; 8.0 – Added Policy Owner section; 9.0 – Added Review Cycle section; 10.0 – Added Summary of Changes section.