Emergency Response Plan Guidance

Issued by: Solano County Office of Emergency Services
530 Clay Street, Fairfield, CA 94533
Contact: 707-784-1600
OES@SolanoCounty.gov

This document outlines the required components to be included in the Emergency Response Plan (ERP) submitted to the Solano County Office of Emergency Services by the owner or operator of a battery energy storage system (BESS) facility within Solano County.

General Instruction	The document must be clearly labeled and include tabbed sections to distinguish each part. If acronyms are used, an acronym list must be provided as an appendix. A glossary should be included to define industry-specific terms and concepts that may not be familiar to individuals outside the industry. For electronic versions of the ERP, embedded hyperlinks should be included where appropriate to enhance document usability during an emergency. The ERP must include a header and footer on each page. **Header Information:** • "Emergency Response Plan" • Facility name and address • 24/7 Emergency Hotline telephone number **Footer Information:** • Page number Physical copies of the ERP must be provided to any emergency response organization upon request. The Solano County Office of Emergency Services must receive three (3) physical copies, along with the digital version upon publication. Physical copies can be mailed or dropped off in person at the address listed above.
Cover Page	• "Emergency Response Plan" • Facility Name, address, and website (if applicable) • Owner/operator name and logo • 24/7 Emergency Hotline telephone number • Date of issue

DRAFT

	• Version number
Table of Contents	Clearly labeled, without the use of acronyms.
Plan Version Information & Record of Revisions Table	• Version: [Version Number] • Date of Issue: [MM/DD/YYYY] • Next Review Date: [MM/DD/YYYY] • Prepared By: [Name of Person/Company Responsible] • Reviewed By: [Name of Safety Officer/Regulatory Body] • Approved By: [Facility Management Approval] • Record of Revisions Table: [Date of Change/Substance of Change/Entered By]
Introduction	• **Purpose:** Define the intent of the ERP—to ensure a timely, coordinated, and effective response to emergencies in order to protect life, environment, and property. • **Scope:** Applicability to all phases of BESS operations (construction, commissioning, operation, decommissioning). • **Assumptions:** Outline any conditions or factors that were assumed to be true when drafting the ERP. • **Regulatory Compliance:** This Emergency Response Plan complies with all applicable local, state, and federal regulations, including: o SB 38 (Emergency Response Planning for BESS) o CPUC General Order 167 o NFPA 855, NFPA 70, NFPA 1 (2021+ editions) o Solano County o Cal Fire & California Environmental Quality Act (CEQA) o EPA Tier II reporting requirements (if applicable)
Facility Overview	• **Facility Contact Information:** o Dial 9-1-1 for any potential life-threatening emergency o Emergency Hotline: [24/7 Hotline Number] o Primary Contact: [Name, Title, Cell Number, Email] o Secondary Contact: [Name, Title, Cell Number, Email] o Facility Operations Center: [Phone Number, Email] o On-site Security: [Phone Number, Email], if applicable • **Site Description:** o Location, zoning, access roads, nearby structures o Description of critical infrastructure o Detailed site maps o Site access procedures for emergency response organizations • **BESS System Details:** o Type of battery chemistry (e.g., lithium-ion, LFP, flow, etc.)

DRAFT

	○ System capacity (MW/MWh), inverters, transformers, HVAC/fire protection systems ○ Safety systems: gas detection, thermal sensors, suppression systems • **Hazard Identification Summary:** ○ Quick-reference table summarizing potential facility hazards (natural and human-caused) • **Detailed Facility Layout, including but not limited to:** ○ Hazard zones ○ Evacuation routes ○ Emergency assembly point(s)
Roles & Responsibilities	**Facility Personnel** Develop a comprehensive list of facility personnel roles and clearly outline the specific responsibilities assigned to each role before, during, and after an emergency. Responsibilities should be aligned with each individual's training, authority, and expected duties during an emergency at the facility. Alternate personnel for each role should be designated to ensure coverage at all times. **At minimum, the following roles must be addressed:** *(titles may vary by organization)* • Emergency Coordinator • Public Information Officer (PIO) • Safety Officer • Remote System Operator • On-Site Personnel **External Partners** Develop a comprehensive list of external partners and agencies that play a role in preparedness, response, or recovery during an emergency at the facility. This list must include regulatory authorities, emergency response organizations, and utility or infrastructure partners relevant to the site and its operations. Responsibilities and obligations should be tailored to reflect the specific size, location, and operational characteristics of the facility. Where jurisdictional ambiguity exists *(e.g., air district or fire authority boundaries)*, ensure both entities are listed. **For each organization listed, clearly outline the following:** • Primary responsibilities during an emergency involving the facility • Situations in which the organization will be notified or involved *(specific communication and notification procedures are addressed in a separate section)*

DRAFT

	• Obligations of facility personnel to support effective coordination *(e.g., providing site access, data, notifications, compliance reporting)* **The following external partners must be considered:** • Fire Authority Having Jurisdiction • Law Enforcement Authority Having Jurisdiction • Solano County Emergency Medical Services (EMS) *(in the event of a mass casualty incident at the facility)* • Solano County Office of Emergency Services (OES) • Utility Provider (e.g., PG&E or local power provider) • Solano County Department of Resource Management, Environmental Health Division (Certified Unified Program Agency (CUPA)) • Solano County Department of Public Health • CAL FIRE *(as applicable based on location)* • California State Warning Center (CSWC) • California Public Utilities Commission (CPUC) • California Department of Toxic Substances Control (DTSC) • San Francisco Bay Regional Water Quality Control Board (RWQCB) • Bay Area Air Quality Management District (BAAQMD) *(if applicable based on location)* • Yolo-Solano Air Quality Management District (YSAQMD) *(if applicable based on location)* • U.S. Environmental Protection Agency (EPA) • California Independent System Operator (CAISO) *(if the facility is utility-scale and directly connected to the transmission grid)* • U.S. Department of Transportation – Pipeline and Hazardous Materials Safety Administration (PHMSA) *(if hazardous materials are transported to/from or stored onsite)* • Occupational Safety & Health Administration (OSHA) *(for worker safety-related incidents with federal oversight)*
Risk & Hazard Analysis	Conduct a comprehensive risk assessment for each of the environmental and human-caused hazards identified below. The intent is to identify vulnerabilities, anticipate cascading impacts, and inform mitigation strategies that improve the resilience and safety of the site. **For each hazard, the assessment must:** • Identify possible initiating events • Evaluate the likelihood and severity of outcomes • Describe potential cascading effects (e.g., fire leading to toxic gas release or grid outages)

DRAFT

	• Outline risk mitigation strategies currently in place or recommended • Include analysis of impacts if the entire facility was compromised, such as, a catastrophic disaster or bad actor involvement (e.g., a cyberattack that forced the entire facility into thermal runaway). Additionally, the assessment must consider the unique characteristics and risk exposures of the site, including environmental, operational, and community-specific factors. Special attention should be paid to: • Known vulnerabilities such as access/egress limitations, nearby critical infrastructure, or previous incident history • Disproportionate risks to at-risk or historically underserved populations, including limited-English speakers, individuals with disabilities, and communities with limited access to emergency services • Potential impacts to FEMA Community Lifelines, including disruptions to energy, communications, health and medical, safety and security, and transportation networks Where feasible, use flowcharts, plain language, and visuals to enhance understanding and clearly communicate the nature and impact of each risk. **Environmental Hazards:** Hazards related to natural or climate-related events that could impact safety, infrastructure, or continuity of operations. • Wildfire • Flooding & Stormwater • Extreme Heat/Cold/Wind • Seismic Activity • Air Quality Degradation **Human-Caused Hazards:** Threats resulting from intentional acts, human error, or technology/system failures. • Vandalism/Trespassing • Sabotage/Terrorism • Cyberattack* • Arson/Explosion/Arc Flash • Active Shooter • Operator Error • Chemical Spill/Toxic Gas Release • Third-Party Accidents (e.g., vehicle strike, utility failure)
***Cybersecurity Specific Requirements**	Cybersecurity review must include any technological systems utilizing an IP connection, regardless of whether the network is considered open or closed. This includes but is not limited to, battery management

DRAFT

systems, energy management systems, supervisory control and data acquisition systems, remote telemetry units, inverters, fire suppression interfaces, and any cloud-based or remote-access components.

As part of the comprehensive threat mitigation strategy, facilities must implement a continuous monitoring and surveillance system capable of detecting and alerting on unauthorized access attempts, logging and retaining events for forensic analysis, and identifying anomalous or malicious activity across connected systems.

Cybersecurity reviews must be conducted at least once annually or following any major system upgrade and documented for compliance purposes.

Required Technical Controls:

- **Role-Based Access Control (RBAC):** Enforce least privilege principles across all user accounts and devices.
- **Multi-Factor Authentication (MFA):** Required for all remote access and privileged accounts.
- **Encryption:** Encrypt data in transit (e.g., TLS 1.2 or higher) and at rest using FIPS 140-2 validated algorithms.
- **Network Segmentation:** Use firewalls and VLANs to isolate critical systems from public or less-trusted networks.
- **Patch and Vulnerability Management:** The cybersecurity ERP must include a documented process for regularly updating software, firmware, and operating systems, including validation of third-party vendor updates, if applicable.
- **Emergency Response Procedure:** The ERP specific to cybersecurity must align with CPUC and NIST guidance.
- **Audit Logging and Retention:** Enable logging on all systems and retain logs in a secure, tamper-evident manner in line with the records retention policy.
- **Backup and Recovery:** Ensure regular, encrypted backups of critical systems, with tested recovery processes.

Regulatory and Industry Standards:
Cybersecurity policies and procedures must align with applicable federal, state, local, and industry standards, including:

- **California Public Utilities Commission (CPUC):**
  - **Rulemaking (R.) 18-12-005:** Addresses physical and cybersecurity threats to electric supply facilities. All BESS operators should align with security expectations under the CPUC's grid safety framework.
  - **Decision (D.) 20-06-017:** Requires regulated utilities to report on cybersecurity risk mitigation efforts and encourages third-party developers to adopt consistent standards.

DRAFT

	• **California Energy Commission (CEC)**:
	  ○ **CEC Staff Report: "Cybersecurity Guidelines for Distributed Energy Resources" (2021):** Recommends baseline cybersecurity practices for grid-connected resources, including authentication, encryption, and update protocols.
	• **North American Electric Reliability Corporation (NERC)**:
	  ○ **NERC Critical Infrastructure Protection (CIP) standards (e.g., CIP-003, CIP-007):** Required for systems directly impacting the bulk electric system.
	• **National Institute of Standards and Technology (NIST)**:
	  ○ **NIST SP 800-82 Rev. 2 –** ***Guide to Industrial Control Systems (ICS) Security***
	  ○ **NIST Cybersecurity Framework (CSF)** – A voluntary framework adopted by many California energy entities for managing cyber risk.
	• **International Electrotechnical Commission (IEC) 62443**:
	  ○ Comprehensive security standards for industrial automation and control systems, applicable to SCADA and similar architectures in BESS environments.

Emergency Response Procedures	Develop detailed response procedures for each identified hazard type, covering the full cycle from pre-event preparation and incident detection to recovery and return to normal operations. Facility personnel must work in coordination with emergency response organizations for the development of evacuation trigger points, shelter-in-place guidance, etc. The emergency response procedures should incorporate a tiered incident classification system to ensure appropriate response levels. Develop a regular and ongoing environmental monitoring procedure to assess potential impacts to life, property, and the environment during normal operations. Baseline data must be collected prior to the start of site construction for comparison. Monitoring must include, at a minimum, air quality (quarterly), water runoff analysis (semi-annually, excluding the rainy season), and soil sampling (annually). Soil sampling must include on-site and contiguous properties. The baseline testing must include data for all chemicals or heavy metals associated with the battery chemistry used at the facility, particularly those of greatest concern to human health, wildlife, property damage, or environmental degradation during thermal runaway or off gassing incidents. *See cybersecurity specific requirements for additional details. Where feasible, use flowcharts, plain language, and visual aids (e.g., diagrams or infographics) to enhance understanding and clearly communicate response procedures.

DRAFT

Training & Exercise	Develop a comprehensive Training and Exercise (T&E) program for all facility personnel—both on-site and remote, and emergency response organizations. All activities must comply with Homeland Security Exercise and Evaluation Program (HSEEP) standards and adopt an all-hazards approach to preparedness. The facility must conduct at least one multi-disciplinary, multi-jurisdictional exercise each year, with a full-scale exercise held at least once every three years. Personnel training must align with the requirements of the State Emergency Management System (SEMS) and the National Incident Management System (NIMS). Additionally, facility personnel are encouraged to attend an "Infrastructure Liaison Officer (ILO) Basic Course" and "Targeting, Sabotage & Disruption of Public Utilities" course. Both are offered by the Central California Intelligence Center (CCIC) or other nearby Fusion Centers. Emergency response organizations must receive training prior to the start of operations at the site. If areas of concern are identified in an After Action Report (AAR) or Improvement Plan (IP), personnel must receive remedial training in those areas within 120 calendar days of the publication of the incident or exercise AAR/IP. An annual T&E calendar must be submitted to the Solano County Office of Emergency Services (OES) within 60 calendar days of its finalization for distribution to the Operational Area emergency response organizations.
Communication & Notification Procedures	Develop communication and notification procedures to support effective internal and external coordination during emergency incidents. Incident communications must align with the Joint Information System (JIS) to ensure consistency, coordination, and accuracy across all responding agencies. While public alert and warning messaging is the responsibility of the local alerting authority, facility personnel must be responsive to requests for information necessary to facilitate proper messaging. Internal messaging to personnel is the responsibility of the facility public information officer, however, must remain in line with the messaging established by the Joint Information Center (JIC). Where feasible, use flowcharts, plain language, and visuals to improve understanding and clearly communicate the size, scope, and risks associated with the incident. **Communication & Notification Procedures must:**

	• Establish internal chains of command for incident notification and escalation. • Outline clear lines of communication, including notification timelines. • Define external notification procedures to local emergency responders, regulatory agencies, and stakeholders. • Include tiered incident classification to guide communication scope and urgency. • Ensure communication procedures support multilingual and accessible messaging. • Work with alerting authorities to pre-develop templates for emergency alerts to streamline response efforts. • Incorporate these procedures into trainings and exercises and regularly review for updates based on best practices and lessons learned.

Documentation & Regulatory Reporting Procedures	Develop clear procedures for documentation, regulatory compliance, and post-incident evaluation to ensure transparency, accountability, and continuous improvement. These procedures must ensure that all emergency incidents, trainings, exercises, and updates are accurately recorded and reported according to local, state, and federal requirements.
	
	Where feasible, use flowcharts, plain language, and visual aids (e.g., diagrams or infographics) to enhance understanding and clearly communicate these procedures.
	
	Documentation & Regulatory Reporting Procedures must include:
	
	• **Record Keeping:**
	  ○ Maintain records of emergency incidents, exercises, and trainings. Records must be maintained in accordance with the established record retention policy.
	  ○ Implement a record retention policy in line with regulatory requirements, such as, EPA Risk Management Plan Rule, OSHA 29 CFR 1910, NFPA 855, and local fire codes, if applicable.
	• **Regulatory Reporting:**
	  ○ Establish reporting procedures for compliance with regulatory bodies (must be in line with response procedures and communication & notification procedures).
	  ○ Ensure submission of required reports within prescribed timelines (e.g., Tier II, chemical release notifications).
	• **Post-Incident Analysis (AARs & Improvement Plans):**
	  ○ Conduct an After Action Review (AAR) within 30 calendar days of any incident that results in (or should have resulted in) activation of this plan and following all

	exercises, as required by HSEEP. A copy of the final AAR must be provided to the involved emergency response organizations, and the Solano County Office of Emergency Services with 30 calendar days of being published. ○ Develop an Improvement Plan (IP) to address gaps and improve response, including identifying responsible parties and timelines, within 45 calendar days of the incident. ○ All data generated as a result of an incident must be submitted in its original form, unaltered, to the County and any other relevant authorities within seven (7) calendar days of the incident. This includes but is not limited to, air quality and gas detection reports, water runoff and soil sampling analysis, battery management system logs, and thermal imaging or IR scan data. ○ To ensure transparency and compliance, all data must be provided in its original form. Any failure to provide complete and unaltered data may be considered a violation of applicable environmental and public safety regulations and could lead to enforcement actions, as appropriate. • **Annual Report:** ○ The owner/operator must submit a comprehensive annual report to the Solano County Office of Emergency Services no later than April 1st of each calendar year. ○ Where feasible, use flowcharts, plain language, and visual aids (e.g., diagrams or infographics) to improve understanding, especially for individuals less familiar with industry-specific terms and concepts. ○ **The report must include, at minimum:** ▪ An overview of any threats made at the site or to personnel (e.g. physical threats, bomb threats, etc.), including the method of contact used, the threat severity, and a summary of the follow up actions taken. ▪ An overview of any cybersecurity threats, attacks, or attempted attacks, including the method of attack, response actions, and any follow up measures taken to enhance security. ▪ An overview of activations of the site security system, fire suppression system, passive fire or explosion detection systems, combustible gas concentration reduction system, and battery management system, including the cause of activation, any follow-up investigations, actions taken, and any adjustments made to systems or procedures.

DRAFT

	▪ An overview of hazardous incidents at the site, including incidents that did not warrant activation of this plan and any follow up actions. Include references to incident reports, if applicable. ▪ An overview of responses by emergency response organizations, including the nature of the response, any coordination with site personnel, and follow up actions taken. ▪ An overview of the trainings and exercises conducted in the calendar year, including the number of offerings, attendance by emergency response organizations or other external partners, and any key takeaways from the trainings or exercises. ▪ Any Improvement Plans generated during the calendar year must be provided as an annex to the report, along with a detailed overview of the corrective actions taken, responsible parties, and any measurable outcomes achieved. ▪ An overview of the ongoing environmental monitoring outcomes, comparing results to the baseline data collected prior to site construction. Any significant deviations from the baseline values must be highlighted, and corrective actions should be outlined. ▪ An overview of the ERP review process, including the participants, frequency of review, the outcome of the review, and a summary of any significant changes made to the plan. ▪ Physical copies of the annual report must be provided to any emergency response organization upon request. The Solano County Office of Emergency Services must receive one (1) physical copy, along with the digital version upon publication. Physical copies can be mailed or dropped off in person at the address listed on page one.
Plan Review & Continuous Improvement	The Emergency Response Plan should be treated as a living document, subject to regular evaluation and enhancement to remain effective, relevant, and compliant. ERP updates may include revisions to procedures, contact lists, flow charts, facility maps, hazard assessments, training and exercise requirements, or any other necessary updates identified during an AAR. Additionally, stakeholder feedback should be sought for plan updates; including organizations listed in this plan as external partners, community organizations, or local residents.

DRAFT

	Review Cycle & Trigger-Based Updates: Conduct a full review of the ERP at least once annually. **Update the ERP in response to any of the following triggers:** • Any incident that results in (or should have resulted in) activation of this plan • Installation of new equipment or control systems • Expansion or modification of the BESS facility • Changes in local hazard profiles (e.g., wildfire risk, climate changes) • Updates to roles, responsibilities, or regulatory requirements • Major organizational changes • Any other changes deemed significant by facility management • Changes in best practice, industry reports, or lessons learned

Annexes & Appendices	• Technical studies conducted prior to site construction and commissioning, including but not limited to:
	  ○ Plume modeling and toxic gas dispersion analysis
	  ○ Chemical composition analysis of fire emissions
	  ○ Runoff water and fire suppression liquid analysis
	• Glossary of industry-specific terms and concepts
	• Acronym list, if applicable
	• Site maps, layouts, and related diagrams
	• Contact lists
	• List of footnoted references, if applicable

DRAFT