ENERGY EXEMPLAR CLOUD OPERATIONS STANDARDS

Contents

ENERGY EXEMPLAR CLOUD OPERATIONS STANDARDS 1
Overview 2
Infrastructure & Physical Security 2
Data Security 2
- Data In Transit 2
- Data At Rest 2

Data Residency 2
Data Privacy 2
Customer Environment 2
Identity, Authentication and Authorization 3
Data Access Controls and Auditing 3
Data Backup and Disaster Recovery 4
Customer Data Retention and Secure Deletion 4
Security Incident Management 4
24X7 Operations Support 5
Application Release and Quality Controls 5
Application Security and Testing 5
Vulnerability & Patch Management 6
Vendor Management 6
AI & Automated Processing 6
Shared Responsibility Model 7
Compliance & Assurance 7
Continuous Improvement 7

Overview

Energy Exemplar's PLEXOS Cloud offerings are ISO 27001 and SOC 2 TYPE II certified and undergoes annual 3rd party audits. To ensure the highest levels of security, compliance, redundancy, and fault tolerance, our Data Centre Operations are conducted with best-in-class infrastructure services from top tier public cloud providers. We operate in geographically dispersed SOC2 TYPE II and ISO 27001-compliant facilities, which are certified in public records by each cloud provider.

Infrastructure & Physical Security

Physical security is provided by the Public Cloud Infrastructure Provider and is audited under their compliance standards. Energy Exemplar has no physical access to any cloud infrastructure.

Data Security

- ### Data In Transit

  PLEXOS Cloud transfers data securely through the industry-standard method Windows Communication Foundation with TLS 1.2 or above encryption. To support back-end integration from your network, Energy Exemplar can provide VPN connections using industry-standard AES (256) IPSec encryptions.

- ### Data At Rest

  Data is encrypted At Rest in the cloud using industry-standard encryption mechanisms.

Data Residency

Customer data is hosted in region(s) aligned with contractual agreements and data residency requirements.

Data Privacy

Energy Exemplar processes customer data in accordance with applicable data protection regulations and contractual commitments.

For more information, please refer to Energy Exemplar's data at https://energyexemplar.com/privacy/

Customer Environment

For each customer, Energy Exemplar establishes a standard and secure tenant environment. Securely housing customer data in a logically separated environment ensures tenant data confidentiality. Additionally, application-specific controls protect data from unauthorized access across multiple layers of application. Diagram 1 shows a complete customer environment setup.

©2026 Energy Exemplar Ltd. Confidential

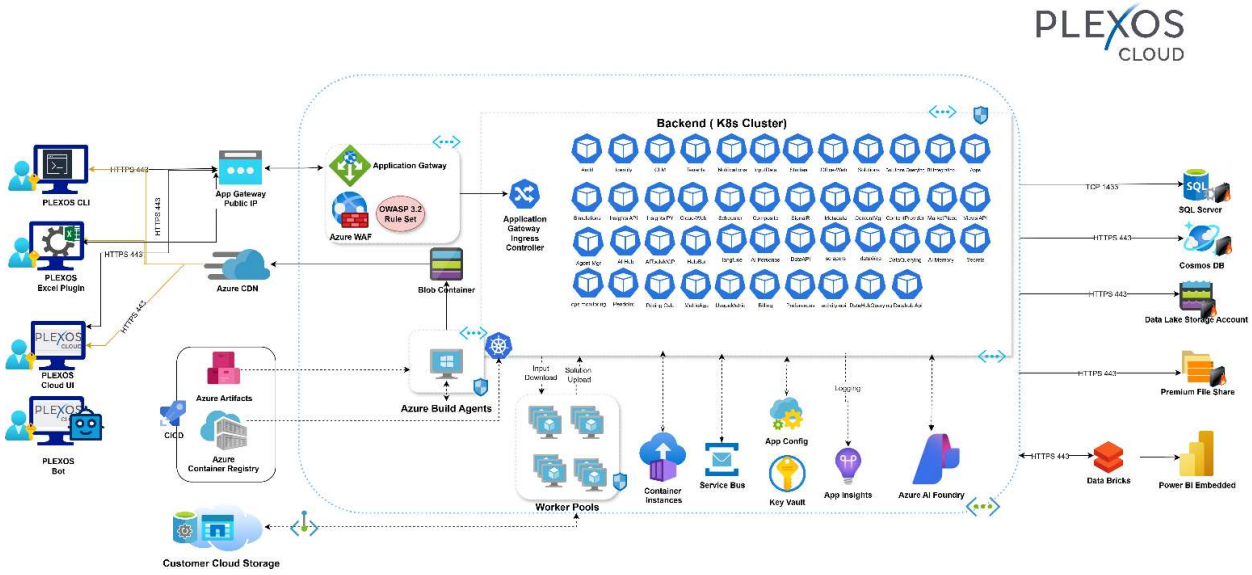


Diagram 1: Customer environment setup

Identity, Authentication and Authorization

All access to PLEXOS Cloud is authenticated and authorized in accordance with strong identity and access management practices.

- Supports local authentication and enterprise identity integration (e.g., Microsoft Active Directory or SAML-based SSO)
- Multi-factor authentication (MFA) is enforced for administrative and privileged access
- Strong password policies and guidelines in line with ISO 27001
- Access to customer data by Energy Exemplar personnel is restricted and governed by:
    - Least privilege principles
    - Role-based access controls
    - Approval-based access workflows
    - Time-bound access where applicable
    - Comprehensive audit logging and monitoring

Data Access Controls and Auditing

Energy Exemplar employees do not have access to customer data by default. Where access is required (e.g., support or troubleshooting):

- Explicit customer authorization may be required
- Access is logged and monitored
- Activities are subject to audit and review

©2026 Energy Exemplar Ltd. Confidential

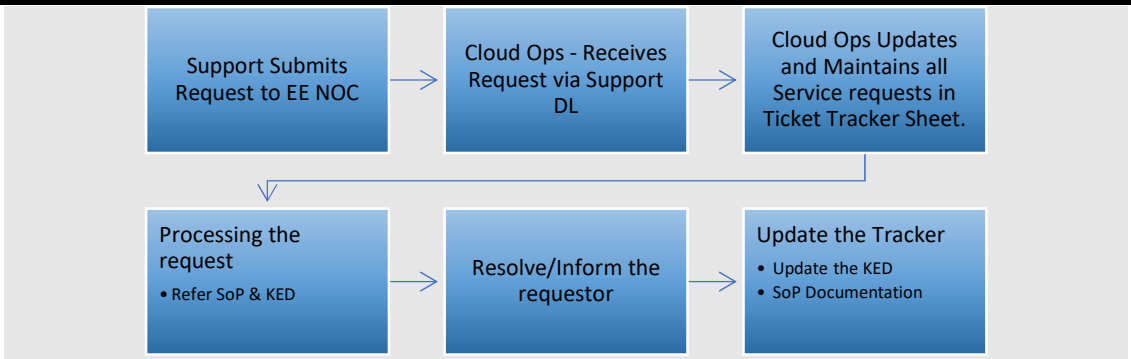


Diagram 2: Access Control Process

Data Backup and Disaster Recovery

The service utilizes the backup services provided by the Cloud Provider. These backups are replicated in multizone which enables restoration of the data (data resiliency).

Overall, the Energy Exemplar's Business Continuity plan covers disaster recovery (DR).

The plan is tested annually or at any time of major architectural changes that warrant the test.

The plan covers customer communication in the event of a DR solution to ensure periodic updates are provided during the event and the customer is kept up to date on the progress of resolution.

A backup and Disaster recovery strategy is designed to support:

- RPO (Recovery Point Objective) of 4hours
- RTO (Recovery Time Objective) of 24 hours

Customer Data Retention and Secure Deletion

Energy Exemplar retains customer data in PLEXOS Cloud for the duration of the subscription. Customers are responsible for downloading or exporting their data prior to subscription termination. Following termination, customer data is securely deleted from production systems within 30 days, and associated backups are deleted within 90 days, in accordance with EE's secure data disposal procedures. A Certificate of Data Destruction can be provided upon written request, confirming completion of the applicable deletion process, subject to legal or regulatory retention requirements.

Security Incident Management

Energy Exemplar operates a 24/7 Security Operations Center (SOC) and incident response processes aligned with industry best practices and SOC 2 requirements.

- Continuous monitoring of systems, infrastructure, and access activity
- Centralized logging and alerting for security-relevant events
- Defined incident detection, response, escalation, and resolution procedures
- Post-incident review and remediation processes
- Customers are notified of confirmed security incidents impacting their data in accordance with contractual and regulatory requirements

©2026 Energy Exemplar Ltd. Confidential

24X7 Operations Support

Our Azure Cloud Infrastructure is managed and maintained by an ISO27001-certified 24x7x365 Operations team. Tier 1 and Tier 2 response is provided by providers onsite NOC staff, for Tier 3 and 4 issues higher skilled staff is on call. Our 24x7 customer responses are regularly audited for quality and adherence to SLA. Executive staff review NOC SLA reports to ensure optimal operations. Additionally, we leverage our Product Support Team for 24X5 Tier 1 product support.

Application Release and Quality Controls

To ensure consistent quality and seamless experience, the development team goes through multiple integrated stages of testing including but not limited to the following:

- Code reviews are performed on all application source changes: All source code is peer reviewed/architect reviewed before merging to ensure security, quality, and consistency.
- Continuous automated testing during the development cycle: Our team runs continuous tests during the development cycle to identify defects early in the development cycle and resolve them early in the development process.
- Backward compatibility testing: We maintain a large repository of models with which we test for backward compatibility and increased model accuracy. Our support and QA teams collaborate with customers to increase this repository of models.
- Security testing: As part of our DevOps release pipeline, we perform static source code analysis for security issues consistent with industry best practices.
- OWASP Top Ten Security testing: Our architects are trained in OWASP security testing and perform security reviews prior to every merge and release.
- Security Penetration testing by independent vendor: PLEXOS is security tested and certified by an external vendor annually.
- Defect Queue Reviews: We perform reviews of the defect backlog internally before every release with a policy to not release with any open severity 1 or 2 issues (major functionality).
- Close monitoring of Escape Defects: Our support team tracks and reports on customer defects after a release to ensure the quality of the release is consistent with expectations.
- Our release process: We have several stages with an open Beta to allow customer exposure late in the development cycle to validate release quality and product performance.

Application Security and Testing

Security is integrated throughout the software development lifecycle in alignment with secure engineering and SOC 2 change management controls.

- Secure code reviews and peer validation
- Automated testing during development
- Static application security testing (SAST)
- OWASP-aligned security testing practices
- Annual third-party penetration testing
- Change management and release controls to prevent unauthorized or insecure deployments

No critical or high-risk vulnerabilities are accepted into production environments

©2026 Energy Exemplar Ltd. Confidential

Security Assessment Approach:

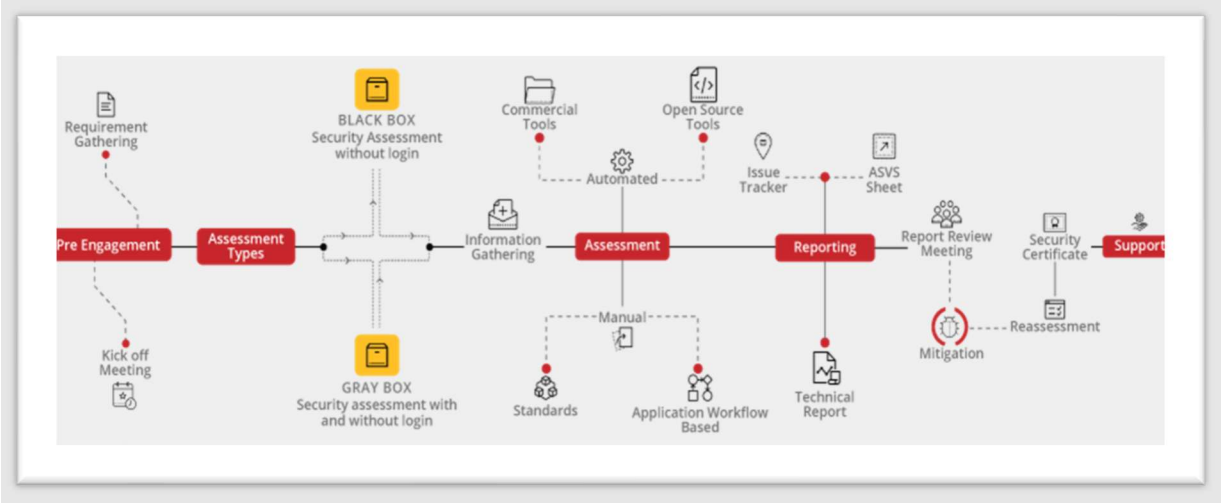


Diagram 3: Security Assessment Approach

Vulnerability & Patch Management

Energy Exemplar maintains a vulnerability & patch management program aligned with industry standards and SOC 2 security controls.

- Regular vulnerability scanning of systems and applications
- Independent third-party penetration testing
- Risk-based prioritization and classification of vulnerabilities
- Timely remediation aligned with severity and risk exposure.
- Periodic deployment of patches
- Tracking and reporting of remediation activities

Security Assurance:

The assessment and reassessment have proven that there are no Critical or High vulnerabilities across the Energy Exemplar Application and API. Further we have met the Secure Application certificate expectations of OWASP, NIST, SANS and CERT-In. The compliance certificate will be awarded with a validity period of one year.

Vendor Management

Energy Exemplar utilizes trusted third-party cloud infrastructure providers. Vendors are subject to security and compliance due diligence. Additional details are available upon request or via Energy Exemplar privacy documentation.

AI & Automated Processing

- Energy Exemplar may use artificial intelligence (AI) technologies to enhance service delivery, operational efficiency, and customer support.

©2026 Energy Exemplar Ltd. Confidential

- Energy Exemplar does not use customer data to train public, shared, or third-party AI models.
- AI processing involving customer data is performed within controlled and secure environments, consistent with EE's information security and data protection standards.
- Access to customer data through AI-enabled tools is subject to established access controls, authorization requirements, and applicable audit logging.
- **Customer Control:** Customers can disable AI functionality within the application if they choose not to use AI-enabled features.
- **Human Oversight:** AI-generated outputs and recommendations are subject to human review and validation. Users retain control over decisions and actions based on AI-generated results.
- **Responsible AI Governance:** EE maintains governance and oversight processes to support the responsible, secure, and compliant use of AI technologies, aligned with applicable legal, regulatory, and industry standards.
- **Transparency:** Where applicable, EE provides transparency regarding material AI usage in service delivery in accordance with contractual and regulatory requirements.

Shared Responsibility Model

- Energy Exemplar is responsible for securing the cloud platform, infrastructure configuration, and application controls.
- Customers are responsible for managing user access, safeguarding credentials, and configuring their environments appropriately.

Compliance & Assurance

Energy Exemplar maintains the following certifications and assurance practices:

- ISO 27001 Certification
- SOC 2 Type II Compliance
- Annual independent third-party security assessments

Continuous Improvement

Energy Exemplar is committed to continuous improvement of its security and operational practices through regular audits, risk assessments, and enhancement initiatives.

©2026 Energy Exemplar Ltd. Confidential