ENERGY EXEMPLAR CLOUD OPERATIONS STANDARDS

Contents

General Operating Stance

Energy Exemplar's 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.

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. A copy of the Provider's compliance report can be provided upon request.

Transport Security

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 (128 or 256) IPSec encryptions.

Data At Rest in the Cloud

All data that is uploaded into the cloud is, by default, encrypted at rest.

Customer Environment

For each customer, Energy Exemplar operations establishes a standard and secure tenant network. Securely housing customer data in a separate network 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.

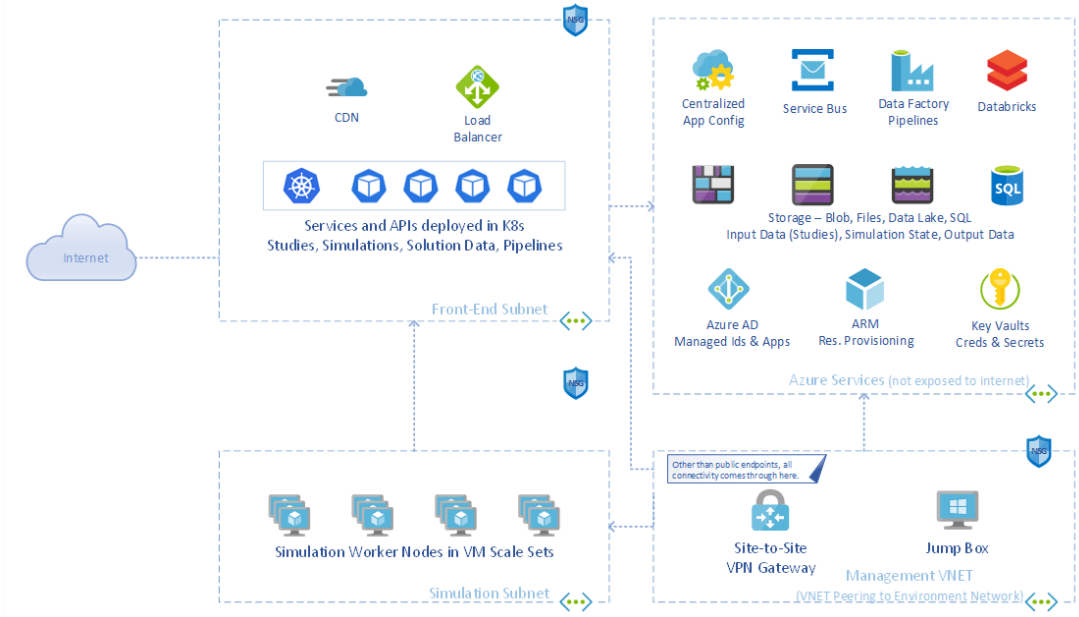

Diagram 1: Customer environment setup

Authentication and Authorization

All access to the Cloud Service is authenticated and authorized. Energy Exemplar offers customers several options to simplify the user login experience without compromising security. We use Local Authentication where passwords are stored inside the Cloud environment, maintained separately from your network credentials. Customers can also choose to integrate with their in-house Microsoft Active Directory.

Data Privacy

Energy Exemplar's data privacy policy can be found at https://energyexemplar.com/privacy/

Data Access Controls and Auditing

Energy Exemplar employees, by default, do not have access to customer data. Access to customer data is restricted. We us several layers of controls for monitoring data access, including administrative and technical controls. Customers may choose to authorize access to support or cloud operations staff for testing or validation purposes.

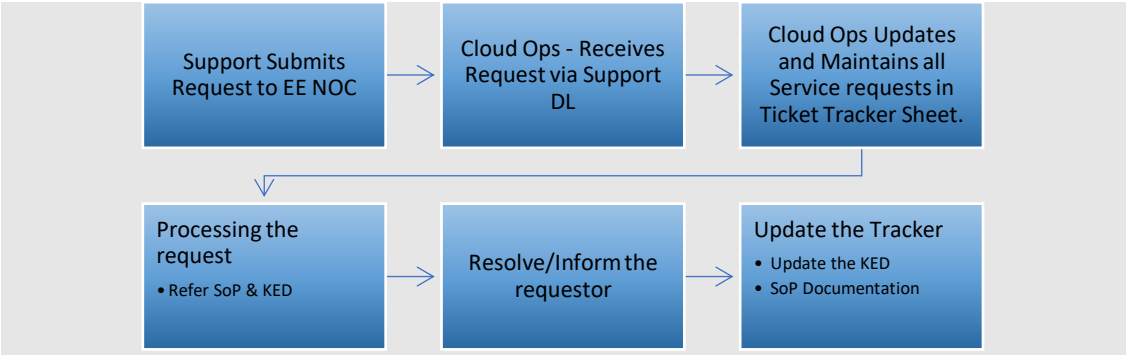

Diagram 2: Access Control Process

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 can be provided upon request after customer onboarding.

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

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 go through 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

Application Security is a strong consideration during every step of our deployment process and ongoing maintenance as well as key steps within our application development and release processes. As standard practice we conduct the annual 3rd party security testing on the application to resolve all high and medium security incidents.

The objectives for Web Application & Application Programming Interface (API) security testing are:

- To verify the input validation functionality of Energy Exemplar application.
- To verify the access control and authentication-related security flaws of Energy Exemplar application.
- To test the security of Energy Exemplar application in its business workflow level.
- To analyze the security of all the API endpoints associated with Energy Exemplar application.
- To analyze whether transactions and all other data of the application are encrypted (both At Rest and In Transit) with updated encryption algorithms.
- To analyze the security of the backend server system of web application portals.
- To identify if the application's database is secure against DB attacks like SQL injection, Graph QL injection, etc.

- To identify whether it is possible to tamper with the transaction amount processed by the application API.
- To identify configuration level security vulnerabilities, present in the web application server and API server.
- To verify that the Access Control Policy is enforced in the Energy Exemplar Application.
- To identify application data breach possibilities with respect to OWASP ASVS.
- To identify if an application is exposing sensitive files like source code, API code, configuration files, etc., to public access.
- To identify if an application has a rate-limiting feature to block Denial of Service attacks.
- To analyze Access logs and identify if logs are exposing sensitive information.

Security Assessment Approach:

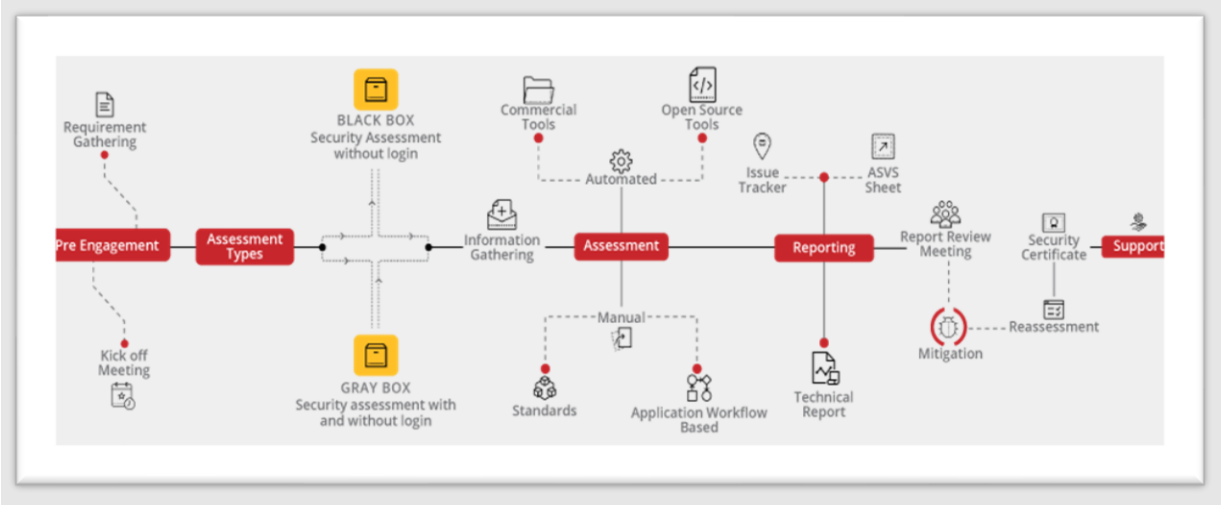

Diagram 3: Security Assessment Approach

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.

Use of Information Technology @ EE:

- ### User Credentials

An account will be created for staff with appropriate access as requested by their reporting/line manager. Login credentials are to be kept secure and are not to be shared with another individual. Staff must change their password when automatically prompted. If an individual believes their login credentials have been compromised, they must notify IT services immediately.

- ### Minimum Password Requirements

EE has implemented strong password policies and guidelines in line with ISO 27001.

- ## Multi- Factor Authentication

All staff, contractors, or third-party vendors who have been assigned an Energy Exemplar email address or access Energy Exemplar platforms are required to have Multi-Factor Authentication enabled. This is an added level of protection in the event user credentials are stolen. Users have the option to configure their mobile numbers to receive a verification code via SMS/TXT or download and install Microsoft Authenticator to their Mobile/Cell Phones.

- ## Email

All emails are tracked and archived for retention and backup purposes. This can only be accessed by Energy Exemplar IT Services in the event of a restore process or security breach, or when requested by a reporting/line manager.

Mimecast's Email Security Platform has been implemented to appropriately protect Energy Exemplar. IT Services receive alerts if a message is in breach of a security policy and can reroute, delete, or block an email message without the end user's knowledge.

- ## Remote Access

Staff who require access to infrastructure, such as but not limited to Local Storage, Testing and Simulation Servers whilst away from an Energy Exemplar office, can remotely connect to these resources via company provided secured VPN connection.

The current approved method of remote access is via VPN client – FortiClient.

Access to local infrastructure via any other connection method is strictly prohibited such as, but not limited to TeamViewer, GoToMyPC, ConnectWise.

- ## Facilities

Energy Exemplar offices require the use of a swipe card/pass to gain access to the premises. Each pass is assigned to a staff member and access to the building is logged for security purposes. Swipe cards/passes are not shared by employees, nor are they allowed to be used by unauthorized personnel.

If a pass is lost or stolen, staff must immediately contact IT Services to have the pass disabled.

For Energy Exemplar offices that use Key access, under no circumstance are keys given out to external parties and or copies made. Each key has a unique number that is assigned to each employee and is to be handed back at the end of their employment at Energy Exemplar.

- ## Company Issued Smartphones

All devices that connect to the Energy Exemplar network and or emails must be password protected.

The operating system on the device must not be tampered with or changed. iPhones are not to be Jailbroken and Android devices must not be Rooted. Only official firmware updates can be applied to mobile devices.

- ## Desk phone – Landline

Staff will be provided a fixed line desk phone if required to perform their role.

Use of landline services is monitored and tracked and may be reviewed as part of an audit, security breach or at the request of a reporting/line manager.

- ## Information Security Awareness Training

Staff are required to undertake mandatory information security awareness training.

- ## Reporting of Security Incidents

It is the responsibility of all employees to report any incident, or suspected incidents, involving a breach of Information and or a breach of IT security where information or data has been externally obtained. These incidents are to be reported directly to the Head of Global IT for investigation without delay.

- ## Portable Storage Devices

Portable storage devices are not to be used unless issued by Energy Exemplar IT Services. Issued USB devices will be encrypted, and passwords are protected to ensure that in the event they are lost or stolen, information is not able to be recovered.

USB ports on all workstations will be disabled for portable storage devices unless it is deemed a requirement for the employee to perform their role. Ports will continue to operate other USB devices.

- ## Loss or theft of Equipment

When a device (laptop, smartphone, iPad) is lost or stolen, the employee must notify IT immediately to report the incident at any time of day or night. The IT department will, among other things, reset passwords and block all access to network resources including email until the issue has been resolved.