ARDEXA

Shared Responsibility Model

Ardexa Digital Control Platform ("Ardexa Platform")

The shared responsibility model is a framework that delineates the distinct and overlapping responsibilities of Ardexa and its customers in managing the Ardexa Platform. This model ensures clarity in roles, enhancing security, efficiency, and performance in renewable energy operations. Ardexa provides the infrastructure and tools necessary for secure and efficient platform operations, while customers are responsible for the data and configurations they manage within the platform.

I. Ardexa Responsibilities

Ardexa is responsible for maintaining the core infrastructure and security of the Ardexa Platform. Key responsibilities include:

- **Platform Security**: Implement security measures to protect the platform's infrastructure, including encryption, intrusion detection, and regular security audits. Ensure the integrity of the platform's core components.
- **Data Management**: Facilitate seamless data integration between remote nodes and the Central Hub, and provide tools for data access, visualisation, analytics and reporting to support customer decision-making.
- **Data Residency**: Ensure that data hosting and back-up is maintained within the specified geographies.
- **Platform Maintenance**: Maintain and update of the Ardexa Platform, including software updates, bug fixes, and performance enhancements.
- **Edge Hardware:** Test and validate that hardware is compatible with Ardexa Platform. Configure hardware sourced by Ardexa, to integrate with the Ardexa Platform
- **Compliance Support**: Provide compliance support tools, such as, access control, data sharing control, audit logs and reporting functions.
- **Technical Support**: Provide support methods and processes for users on a daily basis, including support ticketing, tiered technical support, online documentation and official communication channels.
- **Security Controls for Hosting**: Manage the hosting provider, manage segregation of workgroups, monitor performance of key cloud components and measure hosting performance in each period.
- **Software Updates and Maintenance:** Make available the required software updates. Implement upgrades to software components not managed by Customer.
- **Key Management**: Issue a private key and public certificate to each device on which the Ardexa Agent is downloaded.
- **Data Backup**: Implement data back-up processes and maintain back-ups of all customer data

ARDEXA

II. Customer Responsibilities

Ardexa customers have responsibilities to ensure the effective use of the Ardexa Platform. Key responsibilities include:

- **Data Input and Management**: Provide accurate and complete documentation related to each asset connected to the Ardexa Platform. This includes managing data input, access, retention, and deletion.
- **Data Controls**: Control data sharing and data sharing methods, including user logins, API access, consumer access, etc. Administer duration and auditing of sharing and access.
- **Access Management**: Administer user access and permissions, monitor device connections, and ensure that only authorised personnel have access to sensitive data and platform functionalities.
- **Compliance and Configuration**: Configure the platform to meet their specific operational needs and ensuring compliance with relevant industry regulations. This includes confirming and accepting the design and operation of all control systems.
- **Equipment and Hardware**: Obtain, install, and maintain all necessary equipment, devices, computer hardware, software, and telecommunications services required to access and use the Ardexa Platform.
- **Networks and Connectivity:** Provide Internet access services to all connected devices and covering costs associated with device hardware and site visits, including any devices provided by Ardexa. Customers must ensure compliance with any technical specifications provided by Ardexa and hardware manufacturers.
- **Safety and Testing**: Maintain sole responsibility for outlining required use cases and testing the safety and operational performance of the Ardexa Platform within their environment. They must provide technical resources to ensure installation meets technical, safety, and regulatory standards.
- **Monitoring Data Integrity and Completeness**: Monitor the Ardexa Platform to ensure data is being reliably and accurately collected. Missing data or connection issues may be referred to Ardexa for technical support.
- **Software Updates and Maintenance:** Implement software updates made available by Ardexa, and/or provide permission to implement on behalf of Customer. Follow Ardexa instructions for any updates.
- **Compliance Management**: Monitor and identify where any part of the overall business process needs to comply with regulations and norms. Develop plans, including corrective actions, to ensure regulatory compliance.

III. Shared Responsibilities

Certain responsibilities are shared between Ardexa and its customers to ensure the Ardexa Platform's overall security and efficiency:

- **Security Monitoring**: While Ardexa provides the tools and infrastructure for security monitoring, customers must actively engage in monitoring their data and configurations to detect and respond to potential threats.
- **Incident Response**: In the event of a security incident, both Ardexa and customers must collaborate to address and resolve the issue promptly, minimizing impact on operations.

ARDEXA

IV. Shared Responsibility Model - Overview

Below is a summary of the Shared Responsibility Model

	Ardexa Role	Customer Role	Shared Role
Platform Security	Implement security measures in infrastructure and make available security tools	Implement security tools and monitor non-compliance to policies	Collaborate on monitoring and incident response
Data Management	Ensure performance of data management and back-up systems	Monitor data quality and manage data controls	Collaborate where data collection issues arise
Hosted Platform	Manage hosted application and hosting provider, including cloud software upgrades	Support hosting maintenance and upgrades	Collaborate during maintenance and unplanned downtime periods
Device	Make available and support software upgrades	Implement software upgrades	Collaborate on software upgrade process issues
Compliance	Provide selected compliance support tools	Ensure regulatory and norms compliance	Collaborate to close gaps in compliance
Access Management	Provides tools that enable the Customer to manage users and access permissions.	Administer user access, privileges and audit compliance to Customer policies	Oversee the compliance of users in own organisation
Equipment, Hardware and Connectivity	Validate and configure device hardware to integrate with the Hosted Ardexa Platform	Install hardware and provide connectivity; maintain all equipment	Collaborate where connectivity issues arise
Safety and Risk	Support Customer to implement all risk related corrective actions	Test safety and operational risk	Collaborate to resolve where risk is identified
Digital Certificate and Keys	Make available the Certificate Authority	Manage certificates and keys	Collaborate on incidents and issues