Table of Contents

SYSTEM CONCEPTS 2

Architectural Concepts 2

Security Principles 2

OPERATING ENVIRONMENT 2

Data Center Hosting 2

Network Architecture 3

Service Resiliency 3

Logging & Monitoring 3

Environment Control 4

CUSTOMER DATA MANAGEMENT 4

Data Confidentiality 4

Data Encryption 4

Data Segregation 5

Data Locality 5

Data Access Controls 5

Data Redundancy 6

SECURITY PRACTICES 7

Personnel Security 7

Product Security 7

Operational Security 7

Subcontractor Security 8

INTENDED AUDIENCE AND SCOPE

This document is intended for IT Architects, Quality and Risk Assessors. We provide high-level details about the architecture, security practices, and operating model for the purposes of assessing the fit of the Greenlight Guru Services within your enterprise IT architecture. This document applies to both

Greenlight Guru Quality and Greenlight Guru Ultra eQMS products, which share the same underlying architecture and security practices described herein except where otherwise noted. The document assumes a level of understanding of SaaS and Public Cloud infrastructure.

SYSTEM CONCEPTS

Architectural Concepts

The Greenlight Guru services are operated on a multitenant architecture at both the platform and infrastructure layers that are designed to segregate and restrict access to the data you and your users make available via the Greenlight Guru services.

Greenlight Guru services are web-based. Customers interact with the system through a modern browser application. The web application is built using a service-based architectural style where each internal service is responsible for a non-overlapping subset of the application's processing.

Security Principles

Greenlight Guru strives to maintain the confidentiality, availability, and integrity of data and services by proactively mitigating cybersecurity risks and helping customers meet regulatory demands.

- Risk-based approach - Greenlight Guru focuses on the set of risks it faces and maintaining focus means continually identifying and managing those risks.
- Universal participation - Everyone at Greenlight Guru is actively responsible for the security of our services.
- Least privilege - Users and systems should have the minimum level of access necessary to perform their defined functions.
- Defense-in-depth - Overall security cannot rely on a single defense mechanism. If one security control is defeated, other controls should compensate to resist the attack.

OPERATING ENVIRONMENT

The Greenlight Guru services are hosted over the Internet on a "Public Cloud", which are computing services offered by third-party providers to anyone who wants to use or purchase them. Like all cloud services, a public cloud service runs on remote servers that a provider manages. Greenlight Guru assumes responsibility for the security, availability, and performance of the services we provide, the systems they run on, and the environments within which those systems are hosted.

Data Center Hosting

Greenlight Guru uses the public cloud infrastructure provided by Amazon Web Services, Inc. ("AWS") to host and process Customer Data submitted to the Greenlight Guru services. The production environment

within AWS where the Greenlight Guru Services and Customer Data are hosted are logically isolated in a Virtual Private Cloud (VPC). Customer Data stored within AWS is encrypted at all times. AWS does not have access to unencrypted Customer Data.
Information about the security provided by AWS is available from the AWS Security website. Information about security and privacy-related audits and certifications received by AWS, including information on ISO 27001 certification and SOC reports, is available from the AWS Compliance website.

Network Architecture

Greenlight Guru Services are built on the software-defined networking concepts of the Public Cloud with AWS-specific implementation details. Our networks are built in layers. We use the controls available at each layer to bolster our network's overall security and reliability. Greenlight Guru service runs in multiple independent geographic regions. Each region has one or more Virtual Private Clouds (VPCs) that define a private address space to isolate resources - our private space on the Public Cloud. We further divide the VPC into layers using subnets with access control rules appropriate for the security of the services hosted on those subnets. Each of our network hosts makes use of AWS security groups to limit exposed ports and provide granular access restrictions to discrete resources on the network.

Greenlight Guru uses independent VPCs for each class of environment - from development to production. These independent VPCs strictly limit connectivity between production and non-production environments. The design of our VPCs allows services in one network to only communicate with other services in the same environment level - production can only talk to production. Likewise, Production Data is not replicated in non-production environments.

Service Resiliency

We build our products to best utilize redundancy capabilities, such as availability zones and regions, offered by our cloud service provider. The hosting infrastructure for the Greenlight Guru services spans multiple fault-independent availability zones within geographic regions physically separated from one another.

Each region hosts an equivalent Greenlight Guru service with a distinct network of microservices and data. Access into regional networks and services is only possible from within those same regional networks – e.g. only a service can access another service in that same region. The regional point of service delivery does not have any dependency on other regions and can operate autonomously from each other regions in the event of regional data center failure.

Logging & Monitoring

Systems used in the provision and run of all of the Greenlight Guru services log information to their respective system log facilities which forward logs to a centralized log management service in order to analyze an operating environment. We take care to ensure that no PII or PHI enters the centralized logging system.

Greenlight Guru maintains an extensive centralized logging environment in the production environment which contains information pertaining to security, monitoring, availability, access, and other metrics about

the Greenlight Guru services. The analysis and monitoring of the log event data generate real-time alerts for our service operation.

Environment Control

Greenlight Guru implements and maintains appropriate industry-standard technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, and unauthorized disclosure of or access to Customer's personal data processed or transmitted through the Greenlight Guru services. The Greenlight Guru services have a number of security controls, including but not limited to:

- Multi-Factor Authentication (MFA) - MFA is in use for access to any resource across our AWS environments and enterprise systems that support our products.
- Intrusion Detection - Greenlight Guru employs intrusion detection that continuously scans our network for malicious and anomalous network usage patterns
- File Integrity Management - Greenlight Guru uses file integrity management to keep an eye on critical files and look for unexpected changes to those files.
- Endpoint Management - Greenlight Guru deploys updates and patches to operating systems and key applications across our fleet of laptops and workstations. We have also implemented multiple endpoint protection solutions to protect against threats such as malware.

CUSTOMER DATA MANAGEMENT

We have a number of measures to ensure that we keep customer data secure and customers retain maximum control of their data.

Data Confidentiality

We place strict controls over our employees' access to Customer Data. The operation of the Greenlight Guru services requires that some employees have access to the systems which store and process Customer Data. For example, in order to diagnose a problem you are having with the Greenlight Guru services, we may need to access your Customer Data. These employees are prohibited from using these permissions to view Customer Data unless it is necessary to do so. We have technical controls and audit policies in place to ensure that any access to Customer Data is logged. We do not use Customer Data for any purpose other than providing, maintaining, and improving the Greenlight Guru Services and as otherwise required by applicable law.

Data Encryption

The Greenlight Guru services use industry-accepted encryption to protect Customer Data (1) during transmissions between a customer's network and the Greenlight Guru services; and (2) when at rest. The Greenlight Guru services support the latest recommended secure cipher suites and protocols to encrypt all traffic in transit.

Our current standards are:

- **TLS 1.2+** to protect Customer Data between Greenlight Guru services and our customer's network endpoints.
- **AES-256** to protect Customer Data at rest on persistent storage systems managed and operated by Greenlight Guru.
- Argon-2 hashing algorithm for safe storage of user passwords in the product

We monitor the changing cryptographic landscape closely and work promptly to upgrade the service to respond to new cryptographic weaknesses as they are discovered and implement best practices as they evolve. For encryption in transit, we do this while also balancing the need for compatibility with older clients.

Greenlight Guru uses the AWS Key Management Service (KMS) for key management. The encryption, decryption, and key management process is inspected and verified internally by AWS on a regular basis as part of their existing internal validation processes.

Data Segregation

While our customers share a common cloud-based infrastructure when using Greenlight Guru Service, we have measures in place to ensure they are logically separated so that the actions of one customer cannot compromise the data or service of other customers. We use a concept we refer to as the "org id" to achieve logical isolation of our customers. The context for each tenant is associated with a unique ID stored centrally.

- Each customer's data is kept logically segregated from other tenants when at-rest
- Any requests that are processed have an "org specific" view so other tenants are not impacted

This ensures that one customer tenant cannot access the data of another tenant – nor for one tenant to affect the service of another tenant through their own actions.

Data Locality

Greenlight Guru will store Customer Data at-rest within certain major geographic areas except as otherwise provided in your Order Form. Greenlight Guru services are currently hosted in the following geographic regions:

Greenlight Guru Quality:

- *United States (Oregon)*
- *Germany*
- *Singapore*

Greenlight Guru Ultra:

- *United States (Ohio)*
- *Germany*
- *Australia*

Customer Data stays in a single region and does not move between regions.

Data Access Controls

Protecting Customer Data is a joint responsibility between the Customer and Greenlight Guru. For some of the controls, the Customer cannot configure or disable them; others provide customization of the Greenlight Guru services' security by Customers for their own use.

Service Access Controls are controls that we use internally to protect your data that a Customer cannot configure or disable. At a minimum, Greenlight Guru will align with prevailing industry standards such as ISO 27001 or any successor or superseding standard for managing platform-level access. Greenlight Guru's Service Access Controls include:

- Limited Access - Greenlight Guru strictly limits access to production systems that host Customer Data. Administrative access is granted on a least-privilege basis with a formal "need-to-know" justification. Access is time-boxed and regularly reviewed.
- Strong Authentication - Greenlight Guru requires all admins with access to production systems to have a strong password and use two-factor authentication.
- Limited Authorization - Greenlight Guru admins are only granted access to the resources they need to perform their role or their specific task,
- Audit Logs - Greenlight Guru maintains a complete audit log for platform-level actions performed by our admins.

Customer Access Controls are controls that a Customer Administrator can manage on behalf of their individual organization's usage of Greenlight Guru. These controls include:

- Password Complexity Policy - set password length and character space for their organization to match the enterprise standard.
- Password History Policy - set the rotation period and a number of cycles before a password may be reused.
- Two-Factor Authentication (2FA) - Administrators may configure 2FA for Customer User's as a configuration option for authentication of users to Greenlight Guru services.
- Account Lockout Policy - lock user accounts after unsuccessful login attempts with a Customer Administrator configurable duration.
- Role-Based Access Control (RBAC) - Users are assigned roles and can be configured to sets of more granular access privileges.
- Privileged Action Verification - Greenlight Guru services confirm identity prior to performing sensitive actions to verify the user identity.
- Inactivity Policy - set the lockout of a session after minutes of activity or suspend accounts after days of inactivity.
- Activity Logs - Greenlight Guru maintains an extensive audit log of Customer User actions.

Data Redundancy

Greenlight Guru performs backups of Customer Data hosted on AWS's infrastructure every night. Customer Data backups are retained for at least 35 days. Each backup copy is stored redundantly across multiple availability zones and encrypted in transit and at rest using the Advanced Encryption Standard. Our backups are for use in a major disaster event that affects all or some of the Greenlight Guru services. We have well-tested backup and restoration procedures that allow recovery from a major disaster.

We do not use these backups to revert customer-initiated destructive changes.

SECURITY PRACTICES

Personnel Security

Greenlight Guru ensures all of our staff know how to do their work securely and are empowered to act accordingly.

- Information Security Policies - All of our employees and contract personnel are bound to our policies regarding Customer Data and we treat these issues as matters of the highest importance within our company.
- Background Checks - Background checks are performed, as permitted by local laws, on all new hires to aid in this process. Depending on the role, background checks may include criminal history checks, education verifications, and employment verifications.
- Security Awareness Training - In addition to general information security training, more targeted training is available to our product and engineering teams on secure coding.

Product Security

Product engineering is required to follow security best practices. The product should be "Secure by Design '' and "Secure by Default". Our product and platform engineering teams incorporate the latest security best practices and automate security testing throughout the Greenlight Guru software development lifecycle.

- AppSec Training - All Product Engineering teams must complete application security training annually that includes coverage of current security risks (e.g. OWASP Top 10) and techniques for controlling those risks in our application software
- Environment Segregation - Development, Testing, and Staging environments are logically separated from the Production environment. No Service Data is used in our development or test environments.
- Vulnerability Management - Greenlight Guru maintains controls and policies to mitigate the risk of security vulnerabilities in a measurable time frame that balances risk and the

business/operational requirements. Greenlight Guru uses third-party tools to conduct vulnerability scans regularly to assess vulnerabilities in Greenlight Guru cloud infrastructure

- Penetration Testing - Greenlight Guru engages independent third-party entities to conduct application-level penetration tests. Security threats and vulnerabilities that are detected are prioritized, triaged, and remediated promptly.

Operational Security

We strive hard to build security into all aspects of our day-to-day operational processes. We want security to be an inherent part of how we do our work.

- Configuration Management - Greenlight Guru uses configuration management tools to manage configurations and changes to our infrastructure in our production environments. All infrastructure configurations are maintained as IaC artifacts under version control.
- Change Management - Greenlight Guru follows a change management process that ensures that any change to a production environment has been assessed and de-risked by an independent review prior to release.
- Log Management - Greenlight Guru uses log events to track application usage, system access, and auditable system events. Security logs are collected and analyzed within a log aggregation platform and by System Administrators.
- System Monitoring - Greenlight Guru monitors the health of our service in real-time. We track both technical and application metrics and have the ability to alert Greenlight Guru service administrators through multiple channels when anomalies are detected.
- Incident Response - Greenlight Guru maintains established procedures for managing production support and security incidents.

Subcontractor Security

Where Greenlight Guru engages any third-party suppliers (including contractors and cloud service providers) we are intent on making sure those engagements do not in any way jeopardize our customers or their data.

- Vendor Assessments - Greenlight Guru may use third-party vendors to provide the Services. Greenlight Guru carries out a security risk-based assessment of prospective vendors before working with them to validate they meet Greenlight Guru's security requirements.
- Vendor Agreements - Greenlight Guru enters into written agreements with all of its vendors which include confidentiality, privacy, and security obligations that provide an appropriate level of protection for Customer Data that these vendors may process.
- Vendor Reviews - Greenlight Guru periodically reviews each vendor in light of Greenlight Guru's security and business continuity standards, including the type of access and classification of data being accessed (if any), controls necessary to protect data, and legal or regulatory requirements.

[End of document]

GG eQMS System Architecture & Security Practices (DOC-3348) Ver. 0

Approved By:

(CO-736) eQMS documentation product consolidation

Description

Consolidation of GGQ and GGUL backup verification statements into one document representing our eQMS products. GGUL backup verification statement is now obsolete Adding Ultra product to our eQMS System Architecture and Security Practice document

Justification

Administrative - consolidation

Assigned To:	Initiated By:	Priority:	Impact:
Robin Sterzer	Robin Sterzer	High	Major

Version History:

Author	Effective Date	CO#	Ver.	Status
Cody Dills	September 18, 2026 7:12 PM EDT	CO-736	0	Published