TECHNICAL PAPER

Lighthouse Environmental Monitoring Systems and Regulatory Compliance

Version 01. Rev 02. 8/16/2016

LIGHTHOUSE
WORLDWIDE SOLUTIONS

Lighthouse Environmental Monitoring Systems & Regulatory Compliance.

With the never ending shift towards Quality within the manufacturing of pharmaceutical products it is worth looking at the current requirement of GMP and also 21cfr11 in the context of GAMP 5 requirements. How a Company creates, maintains, retrieves, corrects and controls data can affect product Quality. As far as electronic records are controlled, the FDA's main concern has remained the same since the introduction of 21CFR11 and that is "to safeguard record integrity in order to ensure product quality". Therefore "record integrity and data integrity" is a focus by the FDA during regulatory audits.

What is GMP?

Good manufacturing practices (GMP) are the practices required in order to conform to the guidelines recommended by agencies that control authorization and licensing for manufacture and sale of food, drug products, and active pharmaceutical products. These guidelines provide minimum requirements that a pharmaceutical or a food product manufacturer must meet to assure that the products are of high quality and do not pose any risk to the consumer or public *[Source FDA Good Manufacturing Practices]*.

What is GAMP?

It is both a technical subcommittee of the International Society for Pharmaceutical Engineering (ISPE) and a set of guidelines for manufacturers and users of automated systems in the pharmaceutical industry. More specifically, the ISPE's guide The Good Automated Manufacturing Practice (GAMP) Guide for Validation of Automated Systems in Pharmaceutical Manufacture describes a set of principles and procedures that help ensure that pharmaceutical products have the required quality. One of the core principles of GAMP is that quality cannot be tested into a batch of product but must be built into each stage of the manufacturing process. As a result, GAMP covers all aspects of production; from the raw materials, facility and equipment to the training and hygiene of staff. Standard operating procedures (SOPs) are essential for processes that can affect the quality of the finished product.

GAMP5 was released in February 2008 and it's been over 8 years since its introduction so what has Industry learned in those 8 years and how do you use GAMP 5 when implementing an Environmental Monitoring System and also satisfy GMP and 21CFR11. Let's look at the current 21CFR11 revision from April 2105 *[source FDA website].*

What is 21 CFR Part 11?

Title 21 CFR Part 11 is the part of Title 21 of the Code of Federal Regulations that establishes the United States Food and Drug Administration regulations on electronic records and electronic signatures. Part 11, as it is commonly called, defines the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records

21 CFR Part 11 was initially released in 1997 there was much confusion in the Industry on the implementation and the requirements by manufacturers and vendors. In 2003 the FDA released a Scope and Application update. In 2010 the FDA announced it was going to be conducting a series of inspections in an effort to evaluate industry's compliance and understanding of Part 11 in light of the enforcement discretion described in the August 2003 'Part 11, Electronic Records; Electronic Signatures — Scope and Application' guidance (Guidance). The FDA had firmly laid down it intentions on 21 CFR Part 11 compliance and enforcement. *[Source FDA Website].* Below is a guide to 21 CFR Part 11 Requirements and summary lighthouse qualification coverage. This traceability matrix assists in the design of the Monitoring System and is part of the risk assessment into assisting Customers in selection of suitable software that will mitigate any risks with 21 CFR Part 11 and its application.

21 CFR Part 11 Design Controls Summary

The above Matrix outlines the requirements of 21 CFR Part 11 and where Lighthouse's LMS Pharma achieves validation. There is another validation traceability matrix designed by Lighthouse and this is used to cross reference the Customer URS to the actual design and validation tests (proof) of meeting 21 CFR Part 11 and Customer driven requirements.

What are the Regulatory Requirements for Software Validation?

Software validation is a requirement of the Quality System regulation, which was published in the Federal Register on October 7, 1996. Reference Title 21 Code of Federal regulations (CFR) Part 820 and 61 Federal Register (FR) 52602. Unless specifically exempt in a classification regulation, any medical device software product developed after June 1, 1997, regardless of its device class, is subject to applicable design control provisions and must be validated upon installation and if any changes are made post installation.

To summarize the FDA part 11 requirements, they are outlined as;

- Promote a "risk based" approach to GMP
- System Validation
- Record Copying
- Record Retention
- Audit Trail
- System Access
- System Security

What IS Validation?

Action of proving, in accordance with the principals of Good Manufacturing Practice, that any procedure, process, equipment, material, activity or system actually leads to expected results, ***[Eudralex – Volume 4 GMP Guidelines Glossary]***

"Validation" of computer systems is the process that ensures the formal assessment and reporting of quality and performance measures for all the life-cycles stages of software and system development. Its implementation, qualification and acceptance, operation, modification, requalification, maintenance and retirement. *[PI 011-3 "Good Practices for Computerized Systems in "GXP" Environments" Pharmaceutical Inspection Cooperation Scheme (PIC/s), September 2007]*

In early 2010 there was also a shift of focus on selection of Software and Computerized Systems EUGMP and Annex 11Computerized Systems came into operation 2011.

What is EUGMP Annex 11 Computerized Systems?

First released in 2011 Annex 11 applies to all forms of computerized systems used as part of a GMP regulated activities
Annex 11 is a checklist of non-prescriptive requirements that was adopted by the EU GMP to establish the requirements for computerized systems used in the production and distribution of medicinal products
Good Manufacturing Practice (GMP) ensures medicinal products are produced consistently and controlled to the quality standards appropriate for their intended use and as required by product specifications or marketing authorization. Annex 11 details the European Medicines Agency (EMA) GMP requirements for computer systems. Many USA based Manufactures export to Europe and the FDA are part of PICs so Annex 11 Computerized systems requirement is not just isolated to Europe.

Data Integrity

Fundamental to a Monitoring Systems design is Data Integrity. This is a crucial factor in GMP manufacturing data reliability, data integrity, data security, is the data validated can the data be manipulated? All these question are very relevant to selection of computerized systems. Data integrity is achievable with a robust data governance approach to ensure all data is complete, consistent and accurate. At Lighthouse Worldwide Solutions we design our software AND our hardware to achieve complete, reliable and accurate data. Our APEX line of particle counters were in fact designed to achieve this and our LMS Pharma software has also been designed and validated to prove the data is reliable, secure and accurate.

How do we achieve data integrity at Lighthouse?

At lighthouse we believe in a "quality by design" approach. Firstly, we have designed our software and hardware based on GAMP standards and it is then designed to meet Customer requirements based on a customer driven formal risk assessment, customer URS and a formal design review to verify the software meets customer specifications. At this stage the implementation of standard operating procedures are discussed. 21CFR11 requirements cannot be achieved without Customer driven SOP's.

What do Regulators look for?

- Backdating
- Fabricating data
- Missing data
- Missing comments on alarm acknowledgements
- Sample reruns
- Not recording activities
- Releasing failing product
- Testing into compliance
- Not saving electronic or hard copy data

Design Controls for Data

Quality by Design is the best approach but first you need to apply design controls for your data.

- Identify Critical Data
- Identify risks
- Determine confidence level
- Establish meaningful data reporting
- Establish controls over data lifecycle
- Generate proof (Audit trails, checklists)

Data Integrity Program

A data integrity program is a significant component of a company's Quality System, providing foundational assurance that the data used to demonstrate a company's products are safe and effective for their intended use and are in compliance with regulatory requirements. Below is a summary of such a program outlined by the PDA recently which outlines elements of a code of conduct for data integrity in the Pharmaceutical Industry.

ELEMENTS of a CODE OF CONDUCT FOR DATA INTEGRITY

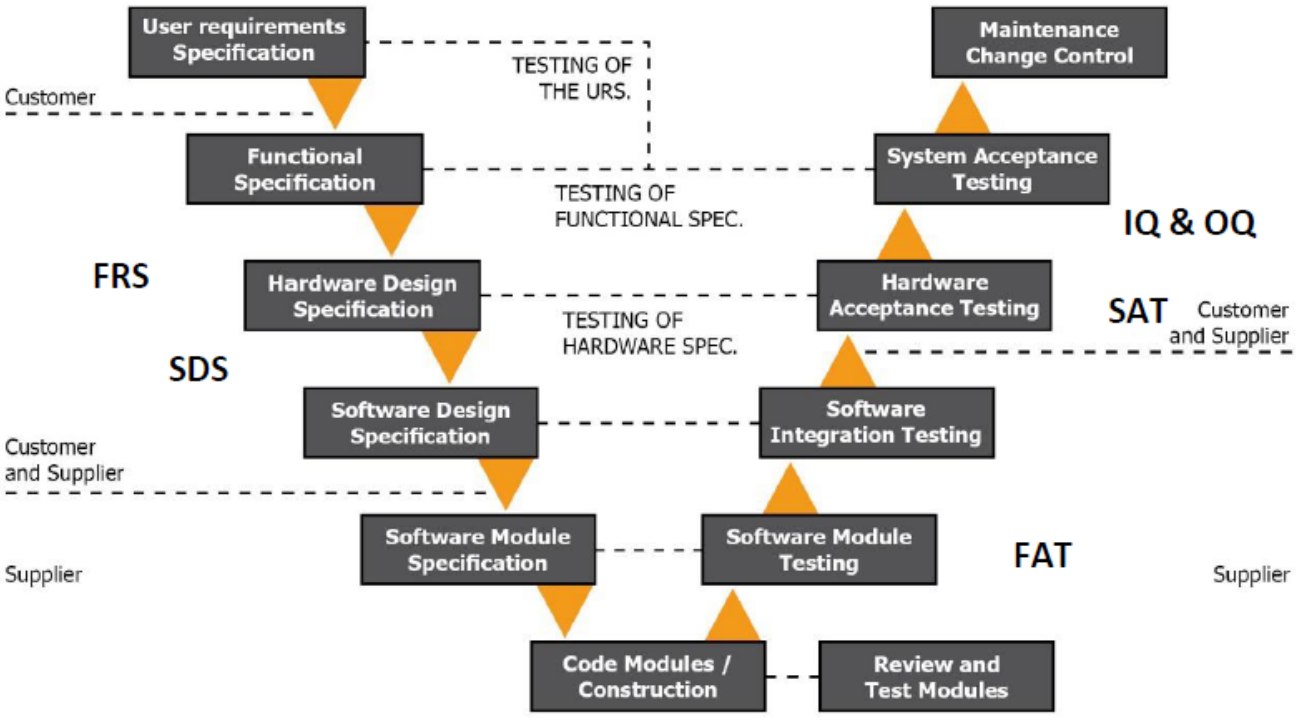
- Applicability
- Data Collection, Analysis, Reporting and Retention
- Electronic Data Acquisition Systems
- Electronic Access Security Measures
- Auditing of Quality System for Data Integrity
- Investigations of Wrongful Acts
- Reporting Wrongful Acts
- Disciplinary Actions for Employees due to Wrongful Acts
- Notifying Regulatory Authorities about Data Integrity Issues
- Data Integrity of Outsourced Services & Purchased Raw Materials
- Employee Training

How does Lighthouse design all of these elements into a Monitoring System suitable for Your Needs? Let's look at a few crucial factors to consider Monitoring System capabilities.

- Must be GAMP designed and developed
- Must meet 21CFR11 requirements with assistance of SOPs
- Must meet EUGMP Annex 11 requirements
- Must have data integrity
- Must be validated
- Must have a Service Level Agreement – Business Continuity

Lighthouse GAMP5 Designed and Developed System

- **Validation Master Plan**
- **Risk Management Plan**
- **User Management Specifications**
- **Vendor Assessment / Audit, Qualification and Acceptance**
- **Functional Description and Specification**
- **Design Specifications**
- **System Installation Qualification**
- **System Operational Qualification**
- **System Performance Qualification**
- **Validation Summary Report**
- **System SOPs and Training**
- **Maintenance, Continuous Monitoring, Change Control and CAPA**
- **Security Measures**



Lighthouse LMS Pharma 21CFR11 Design & Traceability Matrix

21CFR11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification	
11.1		Scope	LWS accepts the purpose and objective of the ruling.	N/A	
11.2		Implementation	CFR 21 Part 11 refers to systems. It is the end user's responsibility to ensure that a system is compliant.	LWS hands over a complete system, implementing Part 11 features providing tools to be compliant.	
11.3		Definitions	No comments.	N/A	
11.10		Closed Systems	Access to a LMS Pharma system must be via a specific user interface, which has access controls.	Access will be controlled via user interface. Administrator will assign users privileges. There will be three levels of users.	
		(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records	Records saved to the LMS Pharma database shall be validated.	LMS Pharma database is run as a closed system in the sense that access to a LMS Pharma system must be via a specific LMS user interface, which has access controls. LMS Pharma database exports information to third party applications, which might be classed as open.	☒ FDS ☒ IQ ☒ OQ
		(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	The LMS Pharma database shall store results in human readable form and/or encrypted form.	The LMS Pharma database can store results in human readable form. The contents of encrypted or SQL databases can be viewed using the report generator. This also provides a means of exporting database contents.	☒ FDS ☒ IQ ☒ OQ
		(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	The data shall be stored in encrypted form in the database.	Data files stored on LMS Pharma can only be accessed and read by authorized personnel with current system security privileges and access.	

21CFR11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification	
		(d) Limiting system access to authorized individuals.	Access to LMS Pharma database shall require a username and password. All user actions involving change of parameters or acknowledgment shall require password verification. Passwords shall be aged.	Access will be controlled via user interface. Administrator will assign users privileges. There will be three levels of users. Log in shall require Operator ID and password verification. User actions involving change of parameters or acknowledgement require password verification. Passwords are required to be changed at a specified interval.	☒ FDS ☒ IQ ☒ OQ
		(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	All user actions involving change of measurement parameters after completion of first sample measurement shall be added to an audit log. Each entry shall be date/time stamped, include the Operator ID, and a description of the user's actions shall be recorded to document alterations.	All user actions can be added to an audit log. Each entry is date/time stamped, has the user ID, a description of the user's action and is labeled to detect alteration.	☒ FDS ☒ IQ ☒ OQ
		(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	This is an end user activity.	Operational Checks are a Customer requirement handled by internal end user Standard Operating Procedures (SOP's) developed by the Customer.	
		(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	Users shall be assigned access to various functions. User actions shall be password protected.	Users will be assigned access to various functions. User actions will be password protected.	☒ FDS ☒ IQ ☒ OQ

21CFR11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification	
		(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Data inputs shall be validated for choice and range.	All data input is validated for choice and range.	☒ FDS ☒ IQ ☒ OQ
		(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	This is an end user activity.	Customer requirement handled by internal end user Standard Operating Procedures (SOP's) developed by the Customer.	
		(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	This is an end user activity.	Customer requirement handled by internal end user Standard Operating Procedures (SOP's) developed by the Customer.	
		(k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Customer shall follow change control procedures as part of the life cycle documentation.	Customer requirement handled by internal end user Standard Operating Procedures (SOP's) developed by the Customer.	

21CFR11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification	
11.30		Controls for Open Systems. Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality	LMS Pharma shall run as closed system in the sense that access to a LMS Pharma system must be via a specific LMS user interface, which has access controls. LMS Pharma shall be able to export information to third party applications, which might be classed as open.	There is an export function which give the user the possibility to export data to a various data formats. It is the Customer responsibility to manage exported data appropriately and to ensure the authenticity, integrity and confidentially of this data.	

21CFR11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification	
11.50		Signature Manifestations (a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature. (b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	(1) Signatures shall show the printed name of the signer (2) The date and time when the signature was executed shall be shown (3) The purpose with the signature shall be shown.	LMS Pharma database records have the described security features. There will be a comment field enabling the user to comment why the change was made where applicable. User comments will capture the user name and when the user made the comment with a date and time stamp. Users can enter the purpose of the signature in the comments section.	☒ FDS ☒ IQ ☒ OQ
11.70		Signature / Record Linking Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	All recorded operator interventions shall include the signature as part of the record.	All recorded operator interventions will include the signature as part of the record.	☒ FDS ☒ IQ ☒ OQ

21CFR11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification	
11.100		General Requirements (a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. (b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual. (c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. (2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	(a) Each electronic signature shall be unique to one individual. Signatures shall not be reused or reassigned. (b) End user activity (c) End user activity	(a) The system administrator will assign accounts. LMS Pharma ensures all current User Ids are unique. The management of User Ids is the responsibility of the end user.	☒ FDS ☒ IQ ☒ OQ

21CFR11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification	
11.200		Electronic Signature components and Controls a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	(a) 1 Signatures shall employ at least two distinct identification components such as identification code and password. (i) First signature in a sequence shall require use of both components Subsequent signings shall be executed using at least one component. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) End user responsibility. (3) End user responsibility.	(a) 1 Signatures will consist of two components, Operator ID and Password. Password will require at least 6 characters. (i) First signature in a sequence will require use of both components. (ii) Subsequent signings will be executed using only one component.	☒ FDS ☒ IQ ☒ OQ
		(b) Electronic signatures based upon biometrics shall be designed to ensure		N/a	

21CFR11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification	
11.300		Controls for Identification code/passwords Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:			
		(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	Operator IDs shall be enforced to be unique.	User IDs are enforced to be unique.	☒ FDS ☒ IQ ☒ OQ
		(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Passwords shall be aged to ensure that they are changed regularly. Any new password shall not be allowed to be the same as the previous password.	Password ageing ensures passwords must be changed regularly. New passwords must be different from the previous password.	☒ FDS ☒ IQ ☒ OQ
		(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	Loss management is the end user's responsibility.	End user responsibility.	

21CFR11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification	
		(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	Transaction safeguards shall be used to prevent unauthorized use of passwords and/or Operator ID´s. Attempts to use unauthorized passwords and Operator ID´s shall be logged and after a given number of failed attempts the user account is disabled.	Failed login attempts are logged in the event log (audit trail). After a given number of failed attempts, a user's account will be disabled until a system administrator enables it.	☒ FDS ☒ IQ ☒ OQ
		(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	Initial and periodic testing of devices that bear identification code. This is an end user activity.	This is an end user activity.	

Lighthouse EUGMP Annex 11 requirements Design & Traceability Matrix

Principal

The introduction of computerized systems into systems of manufacturing, including storage, distribution and quality control does not alter the need to observe the relevant principles given elsewhere in the Guide. Where a computerized system replaces a manual operation, there should be no resultant decrease in product quality or quality assurance. Consideration should be given to the risk of losing aspects of the previous system by reducing the involvement of operators

Annex 11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification
GENERAL				
1.0	**Risk Management** Should be applied throughout the lifecycle of the computerized system taking into account patient Safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of computerized systems.	Lighthouse has developed established Risk Assessment templates that are completed with the end user during the design stage of the Monitoring System.	Risk Assessment Completed URS developed URS Traceability Matrix FDS developed System built – FAT – SAT Then system is fully validated on-site and all validation is traceable back to the URS.	☒ FDS ☒ IQ ☒ OQ

Annex 11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification
2.0	**<u>Personnel</u>** There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.	Lighthouse encourages all mentioned personnel to have an active input into the development, design and controls that go into a Monitoring System.	FDS outlines roles and responsibilities of personnel who use the Monitoring System. Based on duties levels of access are determined. IT play an integral role in Monitoring System design especially when a system goes onto a customer LAN – we encourage and require close cooperation with IT.	☒System Security tested ☒ Personnel are correctly trained on using the system.

Annex 11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification
3.0	**<u>Suppliers and Service Providers</u>** 3.1 When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerized system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous.	Lighthouse provides a full Project Scope detailing the Project roles and responsibilities for the whole life-cycle of the project and also beyond with Service Level Agreements. As for the design an operational considerations Lighthouse engages all Customer Department Manager	Scope of Supply Quality Project Plan	☒ QPP

Annex 11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification
	Suppliers and Service Providers 3.2 The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.	Lighthouse has several audits every year with Major Pharma companies.	Lighthouse System designs are enhanced annually based on constant feedback from Customers.	N/A
	Suppliers and Service Providers 3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.	Lighthouse Monitoring Systems documentation are based on GAMP standards and Customer URS are built into Monitoring Systems designs which are tested and validated.	All validation documentation is submitted to regulated users and system owners for review and comment process.	☒ FDS ☒ IQ ☒ OQ

Annex 11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification
	Suppliers and Service Providers 3.4 Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.	Lighthouse keeps all Audit, Customer Monitoring Systems information on file	N/A	N/A
PROJECT PHASE				
4.0	**Validation** 4.1 The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.	Lighthouse follows the GAMP V model for a systems life-cycle and validation. A Risk Assessment which involves lighthouse will help determine the systems requirements. A subsequent URS shall be developed where the FDS design is based from.	▪ Validation Master Plan ▪ Risk Management Plan ▪ User Management Specifications ▪ Vendor Assessment / Audit, Qualification and Acceptance ▪ Functional Description and Specification ▪ Design Specifications ▪ System Installation Qualification ▪ System Operational Qualification ▪ System Performance Qualification ▪ Validation Summary Report ▪ System SOPs and Training ▪ Maintenance, Continuous Monitoring, Change Control and CAPA ▪ Security Measures	☒ FDS ☒ FAT ☒ SAT ☒ IQ ☒ OQ

Annex 11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification
	Validation 4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.	Lighthouse strongly implements a change control process in all Monitoring System documentation.	Any deviations are recorded in Lighthouse report logs during Validation execution. The deviation report is processed and the deviation is managed to a successful conclusion. All steps are documented right up to close out.	☒ IQ ☒ OQ
	Validation 4.3 An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.	Lighthouse Functional Design Specifications (FDS) outline all aspects of the Monitoring System. Product descriptions, wiring diagrams, process flow diagrams, security access. Every aspect of the system in a GMP environment is outlined.	Lighthouse uses a Transmission List which outlines all instruments connected to the Monitoring System with the IDs, wiring ID, Alarm limits, communication type. The Transmission List is developed and the FDS is developed from the Transmission List (TML).	☒ TML ☒ FDS

Annex 11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification
	Validation 4.5 The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.	Most End users will conduct facility audits to verify that the system development has been done so under a current Quality Management system.	Customer Audit of Lighthouse	☒ Successful Audit outcome
	Validation 4.6 For the validation of bespoke or customized computerized systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.	Lighthouse operates in an ISO 9001 environment and our Software Development follows ISPE guidelines.	Lighthouse has had several facility audits by major Pharmaceutical Companies focusing on software development. URS→FDS→FAT→SAT→IQ/OQ The system is fully tested and validated right up to system handover.	☒ URS ☒ FDS ☒ FAT ☒ SAT ☒ IQ ☒ OQ

Annex 11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification
	Validation 4.7 Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.	Lighthouse develops Test methods appropriate for testing system functionality to include all critical process parameters. Lighthouse does not utilize automated test tools.	Lighthouse IQ/OQ protocols are submitted for Customer review and approval prior to execution.	☒ IQ ☒ OQ
	Validation 4.8 If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.	Lighthouse LMS Pharma has data transfer capabilities once data is transferred outside of LMS Pharma control of data is outside of Lighthouse scope.	Customer's responsibility to control and test how exported data is handled. Lighthouse can verify that the data has been exported unaltered.	N/A

Annex 11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification
Operational Phase				
5.0	**Data** Computerized systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.	Lighthouse Monitoring System software has multiple data export capabilities. All data exported is tested for integrity and authenticity source	LMS Monitoring System software has several data exchange options. •	LMS Pharma output options OPC TCP/IP Modbus RTU
6.0	**Accuracy Checks** For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.	Lighthouse recommends that this is a Customer SOP enforced process	N/A	N/A

Annex 11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification
7.0	**Data Storage** 7.1 Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.	Lighthouse servers are recommended to be located securely in a dedicated IT server room. Access to data in a readable format is via LMS Pharma which is controlled by Security privilege features based on level of access.	Location and accessibility are tested in the IQ. Lighthouse test security features in the OQ.	☒ IQ ☒ OQ
	Data Storage 7.2 Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.	Lighthouse have developed procedures for data backup.	Data backup is tested during the OQ stage of the project for operation and accuracy.	☒ OQ
8.0	**Printouts** 8.1 It should be possible to obtain clear printed copies of electronically stored data.	Lighthouse LMS Software has ability to provide clear reports of data in several formats.	Data reports are tested during the OQ stage of the project for operation and accuracy.	☒ OQ

Annex 11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification
	Printouts 8.2 For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.	Lighthouse LMS Software has ability to provide clear batch reporting.	Batch reporting is tested during the OQ stage of the project for operation and accuracy.	☒ OQ
9.0	**Audit Trails** Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.	Lighthouse LMS Software has built in audit trails, with comments attached.	Audit trail is tested during the OQ stage of the project for operation and accuracy.	☒ OQ

Annex 11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification
10.0	**Change and Configuration Management** When critical data are being entered manually (for example the weight and batch number of an ingredient during dispensing), there should be an additional check on the accuracy of the record which is made. This check may be done by a second operator or by validated electronic means.	Lighthouse LMS Pharma software supports manually entry of critical data for example CFU data after remote air sampling has occurred the addition of CFU results can be entered into LMS Pharma. Lighthouse encourages SOP driven protocols be adhered to for confirmation of correct data entry.	All manual data entry should be driven by SOP protocols where manual data verification is conducted by another qualified person. Such SOP verifications are normally covered by a Customer PQ.	☒ PQ

Annex 11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification
11.0	**Periodic evaluation** Computerized systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.	Periodic Evaluation is a Customer driven check. All Lighthouse Monitoring Systems are handed over in a validated state.	Any Customer changes must be documented through a change control process. The extent of the change must be verified if revalidation is required based on any risks. Lighthouse has supported customers with revalidation activities based on a risk assessment as to the extent of the level of validation required to confidently validate the changes have no impact on the process other than the desired outcome.	N/A

Annex 11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification
12.0	**Security** 12.1 Physical and/or logical controls should be in place to restrict access to computerized system to authorized persons. Suitable methods of preventing unauthorized entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.	Access to Lighthouse Monitoring Systems data is controlled by LMS Pharma security logon authentication. Only users with appropriate security access can have access. Data accuracy is verified against OQ testing and by having sensors calibrated to manufacturer and national standards. Any changes to a system must follow a change control process and the impact of such changes need to be validated.	LMS Pharma security features should be activated, tested and validated during Operational Qualifications.	☒ FDS ☒ OQ
	Security 12.2 The extent of security controls depends on the criticality of the computerized system.	Monitoring Systems in Cleanrooms are critical computerized systems. Lighthouse Software is made compliant with 21CFR11 requirements by validation and introduction of Customer driven SOPs.	Critical aspects of 21CFR11 are tested and Customer develops SOPs to handle Customer related requirements.	☒ IQ ☒ OQ

Annex 11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification
	Security 12.3 Creation, change, and cancellation of access authorizations should be recorded.	Lighthouse Monitoring Software has a built in Audit Trail report all activities by a user are tracked and recorded.	Audit Trail functionality is tested during Operation Qualification.	☒ OQ
	Security 12.4 Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.	Lighthouse Monitoring Systems software is designed to log and also control who has user access. All user activity is recorded with a unique User ID.	User activities are tested during Operation Qualification	☒ OQ
13.0	**Incident Management** All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.	Lighthouse Monitoring Systems have built in redundancies to prevent system failures. If system failures are triggered end users are notified by email, visual alarms or by smart phone/device.	System failures are tested during the Operational Qualification stage of system validation.	☒ OQ

Annex 11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification
14.0	**Electronic Signature** Electronic records may be signed electronically. Electronic signatures are expected to: a. have the same impact as hand-written signatures within the boundaries of the company, b. be permanently linked to their respective record, c.include the time and date that they were applied.	All Lighthouse Monitoring Systems store electronic data which is easily retrievable. All electronic data has associated electronic signatures which are permanently linked by record, user ID and date and time.	Lighthouse tests the acquisition, storage and generation of data reports in the Operational Qualification stage of system validation.	☒ OQ
15.0	**Batch release** When a computerized system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.	Lighthouse Monitoring Systems software have batch recording capabilities. All batch records are linked by electronic signatures and also Batch IDs.	Batch records are tested during the Operational Qualification stage of system validation.	☒ OQ

Annex 11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification
16.0	**Business Continuity** For the availability of computerized systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.	Lighthouse Monitoring Systems have SLA options built in. SLA agreements can significantly impact on the time a system recovers from a breakdown. Lighthouse manages remote support on it LMS Pharma systems. Our technical team can remote in to any system and diagnose and fix issues to reduce downtime. Lighthouse also offers true redundant system servers with a watchdog process which enables a redundant server to take over upon failure of a main server ensuring business continuity.	System redundancy is tested in the Operational Qualification stage of system validation.	☒ SLA ☒ OQ

Annex 11 Section	Ruling	Comment	LMS Pharma - Design Solution	LWS Qualification
17.0	**Archiving** Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.		Achieved Data can only be retrieved through LMS Monitoring System software. Original data will not be effected by system changes.	N/A

How do Lighthouse Monitoring Systems and Lighthouse Products meet all the cGMP and Regulatory requirements and provide you with a custom functioning Monitoring System that is easy to use and works for you and safeguards the accuracy and integrity of your data?

Data integrity – By Design

Lighthouse Monitoring Systems are based on Data Integrity and sensor reliability. Data accuracy, authentication, collection and recording are all fundamental aspects of a Lighthouse Monitoring System. We designed our Apex range of sensors to be "best in class" in the Industry. Our remote particle counter range feature many innovative new designs and are feature packed.

Data Integrity

- Self-Diagnostics
- Laser
- Flow
- Detector
- Accuracy
- Data ID
- Data Buffering

Data Accuracy

- ISO 21501-4 Traceable
- Validation Mode
- Validated Data
- OLED Alarm Display
- Self - Diagnosis

Innovation

- Sloped design
- Sealed Inlet
- Self-Diagnosis
- Smart Bracket
- Local Display
- WiFi Data

ApexR5
Remote
Airborne
Particle Counter

Data Availability

- PC or Server
- Client PC
- Web Browser
- Smart Phone
- Tablet
- Local WiFi

Smart Technology

- SMART Bracket
- No visible connections
- ID based on location
- No swapping errors
- Plug 'n' Play
- Easy service Access
- Waterproof housing

Quality by Design

- Sloped Top design
- Stainless Steel body
- Easy Installation
- Sealed Inlet base
- Easy to wipe-down
- H2O2 VHP Tolerant

Risk Mitigation – Through Innovation

All Lighthouse Apex Particle Counters are designed to enable Risk Mitigation. How? Our Technology reduces Risk through technological advances in our design, components, lasers, functionality and by our innovation. Your data integrity is intact and your particle counter is the most reliable particle counter. Our designs are based on 3 Key Questions: 1. How do I access the integrity of my data? 2. How do I make my data easily accessible? 3. How do I know my Particle Counter is compatible for my environment?

ApexPortable

Portable Airborne Particle Counter

WhatIsMyRisk

Data Viewing

- Large Touchscreen
- Easy Navigation
- Real Time
- WiFi Web Server
- USB Transfer to PC

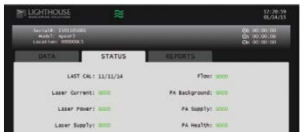
Data Traceability

- View Instrument Status
- Real-Time Data
- Cleanroom Reports
- Smart Phone
- Tablet
- Data when you want it

Web Server

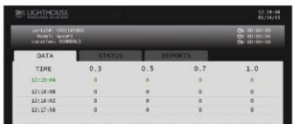
View real time data on your laptop, tablet or smart device.

Web Server - View Instrument Status



Web Server - View Cleanroom Reports

Web Server - View Particle Counts



Secure Data

- Fast
- Reliable
- Secure
- USB Drive
- Compliant

VHP Friendly

- Compatible Parts
- No corrosion
- 304 Stainless Steel
- Protected Sensor
- Standard Feature

Environmental Compatibility

- ISO 21501-4
- Location ID
- Sensor ID
- Self-Diagnostics

Self-Diagnostics – Industry First

Every data record includes a health check of all sensor components. The APEX particle counter range is packed with innovative features to ensure the accuracy and reliability of your data. Every data record packet has several layers of protection to ensure its authenticity. With GMP regulations data integrity, reliability and source is a critical component in decision making process for product safety and release. Be assured with Lighthouse Monitoring Systems and sensors your level of assurance is the highest available anywhere.

Sensor Flow
- Highest Accuracy
- Pressure Compensated
- Flow Alarming
- Auto Laser Shut Off
- OLED Indication
- Status Viewer

Laser Health
- Laser Supply
- Laser Current
- Laser Power
- Calibration
- Alarm Notification

Photo Detector
- Power
- Background Voltage
- Health
- Alarm Notification

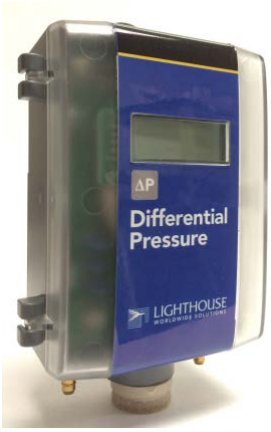
Validation Mode
- Fast
- Reliable
- Secure
- USB Drive
- Compliant

Your Data When You Want It
Seamless Integration over web browser using Wi-Fi connection.

Verified
Every data record is verified through7 diagnostic sensors

Quality by Design
Lighthouse Products

At lighthouse our products and sensors have been built based on the environment they are used in. Apart from particle monitoring, cleanroom room monitoring for pressure and temperature and humidity is just as critical. Pressure is a major parameter to monitor and having the right pressure sensor that has been designed and built with quality and accuracy is critical. Room pressure monitoring ensures the rooms pressure enables a positive or negative status based on the products being processed. TRH monitoring ensures the room environment temperature and humidity are comfortable for workers and that the environment is not suitable for bacterial growth. At Lighthouse we make sure our room monitoring sensors are of the highest quality, accuracy and reliability and they too pack innovative features to ensure your data is accurate and its integrity is intact.



RemoteRTD
Temperature Sensor

Temperature Sensor
- Equipment Monitoring
- Small size
- Easy Mounting
- Traceable calibration
- Integrates to LMS Software
- Quick installation
- Easy Software calibration

RemoteTRH
Temperature and Humidity Sensor

TRH Sensor
TRH-02-15
- Highest RH Accuracy
- New sensor tip protection
- IP65 NEMA Enclosure
- On-site Calibration
- Competitively priced
- Data collection buffer
- Data Redundancy
- Easy Software calibration

RemoteDP
Differential Pressure Sensor

Differential Pressure
- Highest DP Accuracy
- Best Technology
- Display as standard
- On-site Calibration
- Integrates to LMS Software
- Easy to use
- Field selectable ranges

Our Products
- Highest Accuracy
- Best Technology
- Quality by Design
- All USA Manufactured
- All integrate to our Software
- Easy to use
- Intuitive setup

Our Monitoring Systems
- All Lighthouse Products
- 2 Year Warranty
- All Serviced by Lighthouse
- One System for Users
- Easy upgrades
- Redundancy

Monitoring your Cleanrooms – Lighthouse Micro Air Sampling

With the emphasis on manufacture of safe products microbial sampling is a key parameter in any effective environmental monitoring program. Biological and Physical efficiencies are crucial factors to consider and the AC100 has the highest ranking in the Industry. Like our APEX range of non-viable monitoring products Lighthouse has again set the benchmark with our new Active Count 100 Microbiological Air Sampler. We also offer remote air sampling with our Remote Active Count systems which seamlessly integrate into our Monitoring Systems for a complete offering from Lighthouse.

ActiveCount100
Portable Microbial Air Sampler

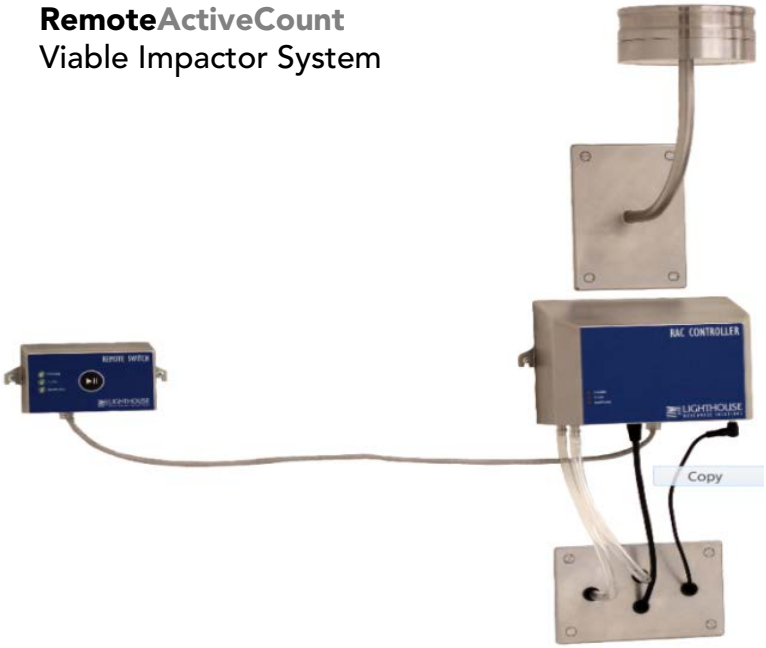
ActiveCount100

- Flow 100 liters / minute
- Best Technology
- Quality by Design
- All USA Manufactured
- 2 Year Warranty
- Easy to use Touchscreen
- Intuitive setup
- Stainless Steel enclosure

Features

- Highest Accuracy
- Best Technology
- Quality by Design
- All USA Manufactured
- All integrate to our Software
- Easy to use
- Intuitive setup

RemoteActiveCount
Viable Impactor System



Remote Active Count

- Remote Monitoring
- Remote start/stop
- Small size
- Easy Mounting
- Stainless Steel Head
- Integrates to LMS Software
- Quick installation

Features

- H 3.5 inch Color Touchscreen
- Intuitive User Interface
- 8 Sample Volumes
- 400 Locations
- Flow Rate Alarm
- 6hrs Battery

Applications

- Pharmaceutical
- Hospitals
- Food & Beverage
- Cleanrooms
- IAQ Air Quality
- Aseptic Manufacturing

Business Continuity – Lighthouse Service Level Agreements

FDA Regulatory regulations in GMP Manufacturing of products require a business continuity plan. Monitoring System designs go a long way in maintaining business continuity through redundant systems and with Vendor after sales support. Critical computerized systems do require outside expert support for maintenance and upkeep. At Lighthouse we offer Service Level Agreements (SLA) covering our full range of equipment. Service Level Agreements maintain your monitoring system or portable equipment providing the data and results on which you have come to rely. Lighthouse SLA Plans are primarily based on (1) Technical Support – Emergency Support (2) Annual Service Support - Planned Support. Annual Service support is quoted separate to Technical Support based on number of sensors and on-site or off-site preferences. There are 3 levels of technical support available. Our remote technical support service requires access to the system over a secure remote connection

SLA Service Support Plans & Resolution with Response Time		
SLA Standard Service	**SLA Premium Service**	**SLA Elite Service**
Technical Support	**Technical Support**	**Technical Support**
Technical Support – Website ticket system to log a technical support request and receive a case no.	Technical Support – Website ticket system to log a technical support request and receive a case no.	Technical Support – Website ticket system to log a technical support request and receive a case no.
Email response within 8hrs	Email response within 4hrs	Email response within 1hr
Technical evaluation within 3 days	Technical evaluation within 1 day	Technical evaluation within 4hrs
Remote assistance within 3 days	Remote assistance next working day	Remote assistance within 8hrs
Remote and Technical support hrs charged per/hr at $160/hr	Remote and Technical support hrs charged per/hr at $130/hr (minimum bundle of hrs required 30/year) **Premium Technical Support Package for $3,900**	Remote and Technical support hrs charged per/hr at $110/hr or $140/hr (minimum bundle of hrs required 50/year) **Elite Technical Support Package for $5,500 excluding weekend support.** **Elite Technical Support Package for $7,000 including weekend support.**
Service Support	**Service Support**	**Service Support**
Annual Service/Calibration **(Prices based on number of sensors)**	Annual Service/Calibration **(Prices based on number of sensors)**	Annual Service/Calibration **(Prices based on number of sensors)**