Canoas, March 30th of 2020

RE.: Sitrad Pro

To whom it may concern,

Sitrad PRO is the new Full Gauge Controls' software for remote management of refrigeration, heating, air conditioning and solar heating installations.

Versatile, Sitrad PRO provides access to installations from the most diverse segments, from supermarket chains, meat-packing plants and restaurants, to hotels, hospitals, and laboratories, among others.

Sitrad PRO continuously evaluates, configures and stores temperature, humidity, time, pressure and voltage data, allowing modification of instrument operating parameters with complete safety and accuracy, from anywhere in the world, via the internet, through a computer or mobile phone. On-demand as well as scheduled reports are available in graph and text format. Real-time alerts are provided in case of out-of-range parameters.

Sitrad PRO has been developed in line with international regulations and requirements and complies with CFR Title 21 Part 11 requirements that include but is not limited to:

CFR Title 21 Part 11 Requirements		Sitrad PRO Compliance
PASSWORD POLICY		
1	Password protected individual user accounts	YES
2	Password and user ID policy (individual unique password and ID, minimum length and strength of ID and password)	YES
3	Choosing password complexity	YES
4	After generation of user ID (user creation) system shall ask for password change on first login	YES
5	Automatically limit number of failed login attempts	YES
6	Automatic logout due to inactivity	YES
7	Automatically log unauthorized login attempts	YES
8	Electronically require users to change password at regular intervals	YES
9	System shall ask to change the password to user periodically by giving prior notification on each login	YES
10	Prevent that a password is being reused	YES

444 Brickell Ave Suite 811
Miami, FL 33131
+1 (877) 917-6643
fullgauge.us

Rua Júlio de Castilhos,250
Canoas/RS - Brasil
+55 51 3475 3308
fullgauge.com.br

	USER MANAGEMENT	
11	User management system and privileges	YES
12	Ensure that the user level based on functionality and authority is defined	YES
13	Facility to create the group such as operator, maintenance, supervisor, manager, etc and allocation of their user privileges can be defined and changed as per requirement at site	YES
14	System shall ask to login and password to change any setpoint/variable value.	YES
15	Ensure that the privileges like delete, copy, cut, paste, rename, etc shall not be allowed to unauthorized user	YES
	ELECTRONIC DATA	
16	Electronic data and report should be human readable and suitable for inspection and review	YES
17	Ensure the content: Performed by with date and time stamp, print by with date and time stamp, system and analysis parameter related information, etc	YES
	ELECTRONIC DATA STORAGE	
18	Generated data shall not be edited or altered	YES
19	Data should be saved automatically to pre defined location	YES
20	Progressive number of cycle or batch should reflect in batch or cycle report	YES
21	Database is fully encrypted	YES
	AUDIT TRAIL	
22	System should track all creations, modifications, and deletions performed in the system (all activities should be logged) with time and date stamp along with user details	YES
23	All critical hardware related errors and warning should be logged in audit trail (system audit trail)	YES
24	User can enter a custom event log to inform an incident	YES
25	Time and date stamp changes automatically, it shall be locked and not editable unless performed by authorized user (shall be defined through user rights distribution)	YES
26	Scheduling of automatic report generation	YES
27	Automatically record identify of individuals who made change	YES
28	System shall prevent to modify or delete audit trail	YES
29	Log when application is updated	YES
30	Selectable option to compel a log text when acknowledging an alarm	YES
31	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 if required at least for 5 years	YES
	DATA BACKUP	
32	Software shall have facility to auto backup to any client or connected central server. Separate path should be provided for backup in SCADA at admin level. Auto backup should be in “Time Series”	YES
33	Email notification in case of backup failure	YES
	OTHERS	
34	User shall not be able to save or relocate the result files, it should be controlled through software only	YES
35	User shall not have rights to create folders or project in software. These rights shall be with administrator	YES