THIRD-PARTY SECURITY REQUIREMENTS DOCUMENTATION

METER Group

ZENTRA CLOUD

The purpose of the Third Party Security Requirements document outlines information on whether or not sufficient security controls are in place at METER Group Incorporated, specifically ZENTRA Cloud, where Third Party groups or Organizations have interest, and to identify if additional controls will be needed in order to achieve compliance with applicable laws, regulations, and Third-Party groups or Organization requirements. The security requirements are designed to vary based on the level of risk the Third Party presents to METER Group Incorporated, specifically guided by the type of information the Third-Party Processes, network connection, services provided by the Third Party, and data availability requirements. METER Group Inc. reserves the right to update this document from time to time.

Additional information not presented in this document may be requested via support.environment@metergroup.com.

Product Name	ZENTRA Cloud
Website Address	zentracloud.com
Product Owner	METER Group Inc.
Website Address	metergroup.com

Contact information	
METER Environment Support	support.environment@metergroup.com

Date of Change	Changes
01/03/2020	Document written
	Document Approved

What is ZENTRA Cloud?

ZENTRA Cloud is a Web Subscription as Service software for ingesting scientific environmental data transmitted by METER Group Inc. cellular enabled Dataloggers.

1. Data Classification

1.1: How is data being collected by, transmitted to, or stored by METER Group	Data is going to be collected and saved locally by a METER data logging device (ZL6) ZENTRA Cloud service allows for this data to be sent to cloud storage and allows monitoring of the data logger and the sensors plugged into it. Elements consist of settings for cell network information on devices (Sim number, APN). Device Information (Batty voltage, Barometer) and attached sensors GPS location, Data logs, Plot information (Customer designation) sensor data (Sensor output)

2. Network Security

2.1: Can you provide sanitized copies of system architecture diagrams and data flow diagrams, as they pertain to the service being provided?	We do not currently provide diagrams of this nature as they expose sensitive architectural elements.
2.2: Do you enforce network segmentation between trusted and untrusted networks (i.e., Internet, DMZ, Extranet, etc.)?	Yes, we do use segmented networks.
2.3: Does METER Group require secure remote connectivity to My Network (or a Third-party network) to access data, or to perform support/administration tasks?	No, we do not require access to your network when using the ZENTRA Cloud system. All data is transmitted over cellular networks from the logger, and the user is interfacing with the presentation of the data in the web browser.

2.4: What protocols will you use to protect application data in transit (e.g., TLS, SSL, SFTP, FTP/S)?	All client to server communications are SSL encrypted

3. Application Security

3.1: Do you follow a formal software development process that includes application security requirements? Please explain.	We follow an internal process that does include discussion of application security requirements.
3.2: Do you use non-production systems to prohibit the storage and use of production data in non-production (e.g., test and development) applications?	No. Our system requires “big data” to function. In order to ensure that your experience in our production system is ideal we perform internal testing and staging on live data sets.

4. Data Storage Security

4.1: Do you purge application data according to a defined data retention schedule? Please explain.	We do not have a defined data retention schedule and retain your data in perpetuity. On occasion we may purge and reprocess your data to correct a processing error.
4.2: How do you secure data in your backups?	All servers and data tables are regularly backed up in an offsite encrypted form.
4.3: How do you ensure that subcontractors and other third parties handle my data securely?	We limit access to your data to internal employees only. No subcontractors, or third parties will have access to your data.

5. Security Policies and Procedures

5.1: Do you have current, documented policies that I can read?	We do not release our security policies to the public.

6. Access Management

6.1: Please describe your process to grant, modify, review, and terminate end-user access to the system.	All user access is managed directly by your organization and Organization Owner/Administrators
6.2: Are you an InCommon Participant, and/or do you support SAML2?	No

7. Change Control and Vulnerability Management

7.1: Do you rely on one or more cloud service providers? If so, please confirm which controls are maintained by you and which controls are maintained by your provider (e.g., patch management, log management).	We utilize cloud providers for functionality such as map drawing, and graphing. However, all controls are maintained by us and not the external providers.

8. Security Assessments

8.1: How often do you conduct regular security control reviews of IT systems (by Internal Audit, a trusted third party, etc.)?	Quarterly
8.2: Do you have a process to address audit recommendations and to ensure compliance with security policies and standards?	Yes. Quarterly meeting with our Security Committee

9. Disaster Recovery and Business Continuity

9.1: Have you activated and tested all or part of your BCP/DRP in the last twelve (12) months? If yes, please describe the scenario and the impact it had on your ability to meet customer service commitments.	We perform regular recovery tests. We validate our backups by performing a restore about once a month. If it is unsuccessful we analyze the issue and fix the problem. When the problem is addressed we rerun the

	restore. The last several have been successful without incident.
9.2: Please explain how you would communicate with Customers during an emergency or an outage.	In general, there is no special outreach in the rare event of a site outage, most customers would not experience disruption at all, In extreme cases, we would reach out to customers. In the event of planned outages, we will notify all customers with as much advance notice as we can. They can reach us through our standard support channels, they will have the same high-quality support that all of our customers receive
9.3: What is your expected recovery time for the services provided to Customers?	Dependent on the nature of the disaster. Most issues we would expect recovery from a disaster in less than 24 hours.
9.4: How often do you assess your operational and environmental risks (e.g., quarterly, semi-annually, and annually)?	we assess operational risks quarterly as part of our quarter planning

10. Public References

10.1: Are other Customers currently using this solution that would be available to contact.	**Kevin Hyde**: Montana Mesonet Coordinator kevin.hyde@mso.umt.edu