Security Statement

LAST UPDATED: JULY 25TH, 2019

This Security Statement applies to the products, services, websites and apps offered by The World Federation for Coral Reef Conservation Inc, which are branded as “The World Federation for Coral Reef Conservation”. We refer to those products, services, websites and apps collectively as the “services” in this Statement. This Security Statement also forms part of the user agreements for The World Federation for Coral Reef Conservation customers.

The World Federation for Coral Reef Conservation values the trust that our customers place in us by letting us act as custodians of their data. We take our responsibility to protect and secure your information seriously and strive for complete transparency around our security practices detailed below. Our Privacy Policy also further details the ways we handle your data.

Encryption

We encrypt your data in transit using secure TLS cryptographic protocols. The World Federation for Coral Reef Conservation data is also encrypted at rest.

Asset Management

The World Federation for Coral Reef Conservation maintains an asset management policy which includes identification, classification, retention, and disposal of information and assets. Company-issued devices are equipped with full hard disk encryption and up-to-date antivirus software. Only company-issued devices are permitted to access corporate and production networks.

Information Security Incident Management

The World Federation for Coral Reef Conservation maintains security incident response policies and procedures covering the initial response, investigation, customer notification (no less than as required by applicable law), public communication, and remediation. These policies are reviewed regularly and tested bi-annually.

Breach Notification

Despite best efforts, no method of transmission over the Internet and no method of electronic storage is perfectly secure. We cannot guarantee absolute security. However, if The World

Federation for Coral Reef Conservation learns of a security breach, we will notify affected users so that they can take appropriate protective steps. Our breach notification procedures are consistent with our obligations under applicable country level, state and federal laws and regulations, as well as any industry rules or standards applicable to us. We are committed to keeping our customers fully informed of any matters relevant to the security of their account and to providing customers all information necessary for them to meet their own regulatory reporting obligations.

Information Security Aspects of Business Continuity Management

The World Federation for Coral Reef Conservation's databases are backed up on a rotating basis of full and incremental backups and verified regularly. Backups are encrypted and stored within the production environment to preserve their confidentiality and integrity and are tested regularly to ensure availability.

Your Responsibilities

Keeping your data secure also requires that you maintain the security of your account by using sufficiently complicated passwords and storing them safely. You should also ensure that you have sufficient security on your own systems. We offer TLS to secure the transmission of survey responses, but you are responsible for ensuring that your surveys are configured to use that feature where appropriate

Logging and Monitoring

Application and infrastructure systems log information to a centrally managed log repository for troubleshooting, security reviews, and analysis by authorized The World Federation for Coral Reef Conservation personnel. Logs are preserved in accordance with regulatory requirements. We will provide customers with reasonable assistance and access to logs in the event of a security incident impacting their account.