EarthCheck's Cyber Security Quick Guide

EarthCheck is committed to safeguarding the information provided to us by our valued customers. In order to provide affective information security, we have the following key technologies in place:

EarthCheck partners with providers with secure systems by design in mind.

We operate with security in mind adhering to the Essential 8 and NIST frameworks

Secure Data Collection

Data Encryption

Secure Systems Design

Industry Security Standards

EarthCheck strives to comply with GDPR requirements, ensuring data is protected as it is collected.

EarthCheck uses data encryption for data storage, ensuring data is protected.

If EarthCheck was affected by a cyber incident or data breach, we follow the below key incident response steps for quick containment of the threat and to limit the potential damage to our client's business.

1. Prepare	2. Detect	3. Contain
EarthCheck regularly conducts security awareness training and phishing simulation exercises to train & lift behaviour of its staff	All IT incidents are treated with urgency including capturing particular key data during the event . These are passed on to the relevant parties efficiently.	EarthCheck takes the necessary steps working with their cyber professionals to ensure that when identified the risks associated with the incident are isolated.

4. Investigate	5. Remediate	6. Recover
Should a cyber incident be reported, appropriate details are collected and provided to the relevant teams to ensure impact is limited.	Once contained and investigations have concluded the cyber incident is eradicated from the network and reoccurrence is prevented.	EarthCheck will work to develop a lessons learnt list to ensure improved processes. Affected systems are restored and new baselines are set.

EARTHCHECK

"Cyber-Security is much More than a matter of IT."