Security and Privacy Policy

ecoPortal is a cloud based, enterprise risk and sustainability management platform developed by Triplics Ltd. and used by organisations internationally. Our platform allows organisations to create content and upload data through their web browsers which is then stored on servers. This document outlines how security is maintained, at a network/hardware, software and data level. These technical security measures are complemented by our privacy policy, which is also described below. A diagrammatic overview of ecoPortal is presented in Figure 1 below.

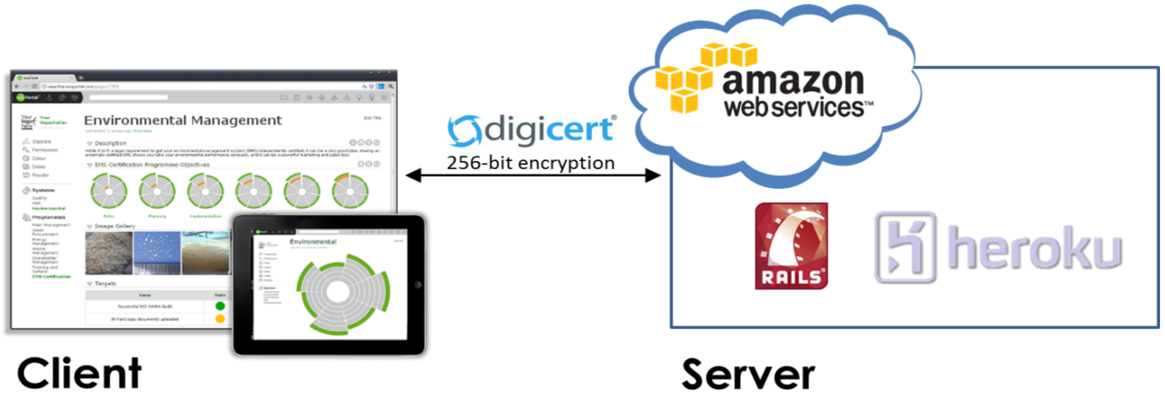

Figure 1. Overview of ecoPortal system

Network/Hardware Security

A. All connections to ecoPortal are encrypted and carried out over 256-bit SSL, preventing man-in-the-middle attacks and information being intercepted by third parties. ecoPortal uses a reputable, world-class vendor for SSL certificates (Digicert), and opts for an extended validation mode certificate for optimum visibility and security.

B. We utilize the Heroku platform (the same services used by Salesforce.com) to ensure that our service has high uptime and redundancy. The Heroku platform is designed to dynamically deploy applications within the Heroku cloud, monitor for failures, and recover failed platform components. Heroku automatically restores our application and databases in the case of an outage.

C. Heroku manages our Network security, which includes utilisation of Firewalls, mitigation of Denial of Service Attacks (DoSA), Spoofing and Sniffing Protection, and Port scanning accessing blocking. More information can be found here: https://www.heroku.com/policy/security

D. ecoPortal and Heroku are built on (and all client data is stored on) the Amazon's AWS (Amazon Web Services) infrastructure, a virtualised computing cloud which has built in safeguards to ensure that information can never leak within the same data centre. As part of this service, Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. Amazon's data centre operations have been accredited under:

- ISO 27001,

- SOC 1, SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II),
- PCI Level 1,
- FISMA Moderate,
- Sarbanes-Oxley (SOX).

E. At Amazon Web Services (AWS) server facilities the physical security controls include but are not limited to perimeter controls such as: fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. Triplics Ltd. offices have similar controls in place such as controlled access points and alarm systems. Triplics Ltd. staff also receive regular training in our security policies and procedures.

F. ecoPortal is set up that in case of a natural disaster centred on our datacentre, ecoPortal is automatically redeployed in other Amazon datacentres.

G. AWS server facilities include numerous environmental safeguards including: fire detection and suppression systems; use of uninterrupted power supply systems (UPS); climate and temperature control; and staff that monitor the servers for electrical and mechanical issues, including performing preventative maintenance. For additional information see: https://aws.amazon.com/security

H. There are both local backups, for instant recovery, as well as periodic off-site backups using Amazon S3. These off-site backups have a minimum of two copies at all times for redundancy. Backups occur daily and we retain 7 daily backups, 4 weekly backups and 3 monthly backups.

Software Security

A. ecoPortal is built using the Ruby on Rails framework which contains built in safeguards against most common web attack vectors, including XSS and SQL injection. We maintain and patch ecoPortal continually to ensure that it remains up to date and secure from announced Common Vulnerabilities and Exposures (CVEs).

B. The core platform for both hosting and our database (MongoDB) is called Heroku (owned by Salesforce). Their security policy can be found here: https://policy.heroku.com/security

C. ecoPortal leverages reputable SaaS (Software as a Service) and PaaS (Platform as a Service) solutions. This ensures that all components of the system are secured, managed and maintained by domain experts. All services employed by ecoPortal run in the same datacenter and as such take advantage of Amazon's robust virtualised platform and its associated security safeguards. These services include Bonsai Elasticsearch, Websolr and MongoHQ.

D. It is Triplics Ltd.’s responsibility to upgrade and ensure the correct working of the overall ecoPortal system.

E. ecoPortal uses an automated dependency vulnerability scanning system from gemnasium.com, to ensure that every component we use is as secure and updated as it can be.

F. Triplics Ltd. understands that attempted intrusions and tests by security experts play a valuable role in ensuring that security holes are identified and quickly closed. To this end, ecoPortal will offer a mirror of the software for testing purposes on request which does not contain any sensitive data. It is against our policy to allow any intrusion attempts or security testing on www.live.ecoportal.com where customer data resides.

G. Triplics Ltd. reserve the right to change and remove functionality at any time. Triplics Ltd. will inform the customers of changes that are relevant to the customer through emails to administrators and change logs on ecoPortal's website. Where necessary, further training will be provided to support the changes.

Data Security

A. Triplics Ltd. management are committed to ensuring the privacy and protection of customer data. This starts at the highest level of the company with directors who understand that security is an essential order qualifier for a SAAS business. In line with this Triplics Ltd. has invested substantial resources in policy, risk management and audit plans in alignment with ISO27001 standards and policies.

B. It is the customer's responsibility to upload and maintain their data, invite and remove people from their system, set and remove permissions on their system, keep passwords safe and secure, and log out of sessions. Triplics Ltd. employees can aid in some of these processes if asked by the customer and also offer training in these activities. Triplics Ltd. also offers a pre agreed amount of support per month for each customer organisation. Beyond this Triplics Ltd. will not access or interfere with any customer data or instance.

C. ecoPortal includes a permission system that gives customer administrators the ability to add or remove users from their organisation, and consequently add or remove their access to the data. Further permissions can be set by customer administrators to limit the access and editing of content on individual pages in the case of internally sensitive content.

D. It is the customer's sole responsibility to ensure that their users, and their content has the correct level of user permissions.

E. Content in ecoPortal can be made publicly accessible through the use of the 'public reports' option offered through the reporting functionality in ecoPortal. This is entirely optional and only users with correct permissions can make content public using this feature.

F. In order to facilitate the invitation of ecoPortal members to organisations, and for ecoPortal members to search for and join organisations on ecoPortal, the organisation names, and user email addresses are not kept private and show up in search results.

G. ecoPortal does not store passwords in their original form. Passwords are irreversibly hashed with a unique salt per-password using the bcrypt algorithm with a high number of stretches to mitigate brute force attacks.

H. ecoPortal does not have automatic logout functionality. All logged in sessions of the ecoPortal software should be attended at all times. Session security is solely the responsibility of the customer.

I. Uploaded files on ecoPortal are stored using Amazon's S3 (Simple Storage Service) and are encrypted at rest. All communications with S3 are encrypted over SSL. To illustrate this, if you were to upload a file to ecoPortal and then subsequently download it, the workflow would be as follows:

i. ecoPortal provides you with a policy document allowing for direct upload to S3 with a restricted key prefix to prevent overwriting of existing data.

ii. Your browser encrypts and transmits the desired file to the S3 service, where it is decrypted upon receipt and immediately re-encrypted with a different key, then stored. The keys to this encryption are stored upon separate, Amazon owned and operated servers. This prevents physical theft of your files.

iii. ecoPortal moves the file into a secure prefix.

iv. Your browser then requests to download the file via an action on ecoPortal itself which ensures that you have the correct level of permissions to access that file. If these checks pass, ecoPortal uses the S3 API to generate a one-time-only expiring URL for you to download the file and redirects you to this URL.

v. Your browser negotiates an SSL connection with Amazon's S3. S3 pulls the file, decrypting it on the fly from the at-rest encryption. The file is immediately re-encrypted and transmitted to your browser. Streaming file transfer ensures that the entire file is never fully decrypted at any given time.

Incident Management

A. If a client becomes aware of an incident, it is their responsibility to notify Triplics Ltd. Communication of security incidents, vulnerabilities or suspected security incidents should be made to Triplics Ltd at issues@ecoportal.co.nz.

B. It is the client's responsibility to act on and remediate all known security incidents within their organization which could compromise their security on the ecoPortal platform.

C. It is Triplics Ltd's responsibility to act and remediate on all known security incidents with the ecoPortal Service.

D. Triplics Ltd. is responsible for categorisation and remediation of incidents. The nature and priority of an incident will internally decided and handled appropriately. For example, any form of data breach would be given high priority. The handling of incidents is as follows:

   i. High priority incidents are triaged and sent to the appropriate team and resolved within 24 hours when possible,

   ii. Medium priority incidents are remedied within 3 days,

   iii. Low priority incidents are resolved within 14 days.

E. If Triplics Ltd. becomes aware of any unlawful access to any customer data stored on ecoPortal's equipment or in ecoPortal's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of customer data (each a "security incident"), ecoPortal will promptly:

   i. Notify the customer of the security Incident within 24 hours,

   ii. Investigate the security incident and provide affected Customers with detailed information about the security incident and what is being done to address them,

   iii. Take reasonable steps to mitigate the effects and to minimize any damage resulting from the security incident.

F. After the event of a security incident, Triplics Ltd. agrees upon request, to provide time stamped audit logs and forensic snapshots to help the customer perform their own internal investigation

G. Triplics Ltd. will provide information to enable the customer to cooperate with requests from investigation by a regulatory body

H. It is Triplics Ltd. responsibility to, when possible, provide restoration of data and services after an incident

J. Triplics Ltd. maintains a specialist information technology indemnity insurance policy (iTech Information Technology Policy) that has been designed specifically for information and communication technology (ICT) service providers by Dual New Zealand. The limit of this insurance is $2,000,000.

Privacy Policy

a) Customers own their data. Unless the customer explicitly marks their data as public, no ecoPortal users other than those specifically invited by the customer can access a customer's data. Triplics Ltd. staff will not review, share or distribute any customer data except in cases explicitly outlined in the 'Software License Agreement', or as may be required by law. Software License Agreements (while customised) outline that customer data will be used only for the purposes of providing services, or preventing or addressing service or technical problems.

b) Triplics Ltd. can view usage statistics for the purpose of improving the usability and system design. All usage information is securely stored and only accessible by authorised Triplics Ltd. staff members.

c) Triplics Ltd. Staff do not have access to customer passwords and will never ask for them. Customers are solely responsible for the security of their passwords, and should never share them for any reason.

d) Customers can opt out of all automated email communications from ecoPortal through changing their ecoPortal digest settings.

e) Triplics Ltd. has the right to change these policies and security settings at any time, which will come into effect when the changes are communicated to all clients by email, or posted online on the ecoPortal website.

f) It is the customer's responsibility to maintain awareness and compliance with ecoPortal published security policies, and applicable regulatory requirements

g) Triplics Ltd. will not disclose customer data outside of Triplics Ltd. or its contracted third party service providers except where directed by the customer, or required by law.

h) Triplics Ltd. will not disclose customer data to law enforcement agencies unless required by law. Should a law enforcement agency contact Triplics Ltd. with a demand for customer data, Triplics Ltd. will attempt to redirect agency to request that data directly from customer. If compelled to disclose customer data then Triplics Ltd. will promptly notify the customer and provide a copy of the demand unless legally prohibited from doing so.

i) Upon receipt of any other third party request for customer data (including the customer's own end users), Triplics Ltd. will promptly notify customer unless prohibited by law. If Triplics Ltd. is not required by law to disclose the customer data, Triplics Ltd. will reject the request. If the request is valid and Triplics Ltd. could be compelled to disclose the requested information, Triplics Ltd. will attempt to redirect the third party to request the customer data from the customer.

j) If a request for customer data is made directly with our third party hosting provider AWS, then the request will be processed based on AWS's policy which states "AWS err on the side of protecting customer privacy and is vigilant in determining which law enforcement requests we must comply with. AWS does not hesitate to challenge orders from law enforcement if we think the orders lack a solid basis."