EC4P Information Security Policy

1.1 Introduction

Thinkstep Compliance Ltd (hereafter 'Thinkstep') own and operate the Environmental Compliance 4 Products (EC4P) cloud based reporting platform. EC4P is designed and implemented to achieve the highest commercial data security standards. In particular, EC4P complies with recommendations and best practices outlined in guidelines provided by the Open Web Application Security Project (OWASP) (ANNEX I).

This Information Security Policy provides an overview of the systems and processes Thinkstep have put in place to ensure safe and secure transmission and storage of all client data within the EC4P system.

2.1 Administrator access restrictions and data transfer

Administrator access to the EC4P system is restricted to security-approved staff at Thinkstep. These staff have received appropriate privacy and data security training.

Thinkstep treats all client data as strictly confidential and undertakes not to in any way sell, (sub-) license, transfer (except where required), or otherwise commercially exploit any client data that has been input into the EC4P system. Where the transfer of data to other organisations is required by law (client product sales data only), Thinkstep will ensure this data is transferred in accordance with the relevant national regulations and data security best practices.

2.2 User Password Security

2.2.1 Password Requirements

Passwords used for EC4P user authentication must pass the following criteria before they are validated and accepted for use:

- → Be at least 6 characters in length
- → Contain at least one upper case letter
- → Contain at least one lower case letter
- → Contain at least one numerical character

To prevent the use of malicious "brute-force" password hacking software, EC4P throttles authentication attempts. Users are prevented from logging in for a period of 10 minutes if they fail to provide the correct credentials after more than five attempts. The throttling is unique to the user's username, e-mail address and their IP address.

2.2.2 Password Hashing Encryption

The conventional method of using a MD5 or SHA1 to generate password hashes is insufficient for modern security requirements. Instead, passwords stored in the

EC4P database are encrypted using a "bcrypt" function which removes password security vulnerabilities by implementing a one-way hash whereby user passwords are never stored in their original format within the EC4P database.

2.3 Web hosting and web server security

EC4P is hosted on servers provided by DigitalOcean, Inc. (DigitalOcean) (www.digitalocean.com). DigitalOcean is an American cloud infrastructure provider which in December 2015 was the second largest hosting company in the world in terms of web-facing computers. DigitalOcean servers are used by more than 30,000 companies including HP, Xerox, Salesforce and Atlassien.

DigitalOcean servers are leased from many third-party data centres around the world. EC4P is hosted at DigitalOcean's London based data centre (LON1) which is provided by Equinix (www.equinix.co.uk). The LON1 facility is compliant to several security certifications and third-party audit programs including:

→ **SOC 1 Type II:** The report covers the detailed controls that the LON1 data centre operates along with an independent auditor opinion about the effective operation of those controls.

→ **ISO 27001:** The LON1 data centre has achieved ISO 27001 certification of the Information Security Management System (ISMS) covering infrastructure, data centres, and services.

→ **PCI-DSS:** The LON1 data centre has been independently validated to comply with the PCI Data Security Standard as a shared host service provider.

2.4 The green padlock (HTTP encryption via SSL)

EC4P uses TLS 1.0-1.2 & SSL 2-3 encryption protocols to prevent any eavesdropping or tampering of data which is transferred between the EC4P web server and any requester client using HTTPS (web browser, another web-application etc.).

Data transfer encryption is achieved using an A rated "Lets's Encrypt" Certificate (SHA256 with RSA). Using Let's Encrypt allows EC4P to benefit from automated quarterly certificate renewal which significantly increases the security provided by SSL certificates. An explanation of the TLS/SSL protocol can be found in ANNEX II of this document.

2.5 Web application level security

EC4P complies with recommendations and best practices provided by the Open Web Application Security Project (OWASP) (ANNEX I).

2.5.1 SQL Injection

Prepared PDO statements are leveraged and input data is validated against the required type at a client, server and database level. All user input is sanitised when passed to the EC4P server.

2.5.2 Cross-site Request Forgery (CSRF)

CSRF tokens are used to ensure third-parties cannot transmit unauthorised requests to any EC4P web end-point.

2.5.3 Cross-site Script Attacks (XXS)

Input data is validated against the required type at a client, server and database level. All user input is sanitised when passed to the EC4P server as input and is escaped (removal of HTML entities) by default when being rendered as output.

2.5.4 Direct Object Referencing

Only resources which are owned by the currently authenticated user can be reached or manipulated through available user end-points. Checks to verify ownership are conducted on every request cycle.

2.6 Penetration testing schedule

EC4P is tested with a range of penetration testing software products on a bi-annual basis. Software used to conduct penetration tests includes but is not limited to: Arachni, OWASP Zed Attack Proxy and SkipFish.

2.7 Backup procedures and data retention

The integrity of data pertaining to the EC4P reporting platform is ensured at various stages and levels within the overall web application and systems architecture of the platform. A non-exhaustive list of data backup and retention procedures is provided below:

→ **DigitalOcean "Droplet" Backup:** Snapshots and Backups (images) are automatically run on a weekly basis and are stored on an internal non-publicly visible network on NAS/SAN servers. Thinkstep manage directly how many regions in which the EC4P snapshots exist and this allows Thinkstep to increase the redundancy of the files that are stored in the backend.

→ **MySQL Database Backup:** Snapshots and Backups (images) of EC4P production databases are run automatically every day and are stored via secure stream transfer to Amazon Web Services (AWS) Simple Storage Service (S3) where they are held privately with no public access for a period of at least one year. AWS S3 is compliant to the ISO 27001, PCI DSS and SAS70 Type II security certifications and third-party audit programs.

ANNEX I

Open Web Application Security Project (OWASP) Guidelines

OWASP Top Ten Project
OWASP Testing Guide
OWASP Risk Rating Methodology

ANNEX II

Explanation of the TLS/SSL protocol (HTTPS)

HTTPS (Hypertext Transfer Protocol Secure) encrypts all information sent and received. An overview of the main processes in HTTPS is provided in the infographic below.