



Crises Control Cloud Security Principles

TRANSPUTEC

Classification: Internal – version 2.4 - 04/01/2021

Transputec provides ICT Services and Solutions to leading organisations around the globe.

As a provider of these services for over 30 years, we have the credibility and sustainability to support businesses with their IT systems and support requirement.



Crises Control Cloud Security Principles

Contents

Introduction	3
Cloud Security Principle 1 - Data in transit protection	4
Cloud Security Principle 2 - Asset protection and resilience	4
Cloud Security Principle 3 - Separation between consumers	5
Cloud Security Principle 4 - Governance framework	5
Cloud Security Principle 5 - Operational security	5
Cloud Security Principle 6 - Personnel security	6
Cloud Security Principle 7 - Secure development	6
Cloud Security Principle 8 - Supply chain security	6
Cloud Security Principle 9 - Secure consumer management	7
Cloud Security Principle 10 - Identity and authentication	7
Cloud Security Principle 11 - External interface protection	8
Cloud Security Principle 12 - Secure service administration	8
Cloud Security Principle 13 - Audit information provision to consumers	8
Cloud Security Principle 14 - Secure use of the service by the consumer	9

Crises Control - Cloud Security Principles

Introduction

Transputec, as a data controller and data processor is fully compliant with the provisions of UK law on data security, which are set out in the EU General Data Protection Regulation, as are our suppliers. Transputec has in place technical and organisational measures in relation to the processing of protected data to ensure that it meets the requirements of GDPR and protects the rights of data subjects.

The Crises Control infrastructure, application and service stack is as follow:

Crises Control Stack	Responsibility
1. Telephony	Twilio
2. App	Crises Control security
3. Website	Crises Control security
4. Middleware/API	Crises Control security
5. OS	Crises Control security
6. Hypervisor	Data Centre security
7. Hardware	Data Centre security
8. Network	Data Centre security
9. Data Centre	Data Centre security

Our hosting partner, Coretx (C4L) is ISO 27001 certified and provides services to multi-national companies and City financial institutions, as well as to numerous local authorities and health organisations and provides our secure data centre hosting. Coretx is fully compliant with the Cloud Security principles.

Telephony security is covered in the Twilio - whitepaper embedded below.



Twilio is ISO/IEC 27001:2013 certified, is on the EU/US privacy shield framework and has recently successfully completed its SOC2 Type II audit for the Trust Services Principles of Security and Availability and hosts its services on Amazon AWS.

The Coretx hosting covers points 6 to 9 of the above Crises Control stack. This document covers points 1 to 5 above.

How Crises Control is addressing the Cloud Security Principles

Cloud Security Principle 1 - Data in transit protection	
Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.	<ul style="list-style-type: none"> ✓ Crises Control is hosted in two ISO 27001/27017/ 27018/20000/9001 accredited data centres- Park Royal and Milton Keynes. ✓ Traffic between data centres is protected using dedicated lines. ✓ SSL certificates encrypt data in transit. ✓ CloudFlare virtual firewall protects the website and app portal. ✓ We control our own physical firewalls at the data centres to meet the maximum-security standards covering all network devices such as firewalls, routers, and switches. ✓ High-level malware and anti-virus defences implemented. <p>Telephony</p> <ul style="list-style-type: none"> ✓ Twilio provide our Telephony services. Twilio's infrastructure is hosted in multiple data centres, utilising state-of-the-art practices for fault tolerance at each level of system infrastructure, including power, cooling and backbone connectivity. ✓ If disruption events occur, Twilio's software is architected to detect and automatically route around these issues in real time to ensure a consistent customer experience. ✓ Twilio hosts its services on Amazon AWS.
Cloud Security Principle 2 - Asset protection and resilience	
Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.	<ul style="list-style-type: none"> ✓ Physical security of the Data Centre and Infrastructure is ISO 27001 certified. ✓ Secure configurations for hardware and software on mobile devices, laptops, workstations and servers. ✓ Asset identification and tagging is enforced. ✓ Regular asset audits take place. ✓ Asset monitoring and control software is deployed. ✓ Limitation and control of network ports, protocols and services. ✓ Regular testing of asset protection and resilience. ✓ Automated failover to second data centre.

Cloud Security Principle 3 - Separation between consumers

Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another.

- ✓ Consumer data and services are logically separated on a shared platform.
- ✓ Penetration tests are conducted after each update of the application.
- ✓ Immediate remedial action is taken if necessary.
- ✓ Application software security is deployed at all times.
- ✓ No banking or credit card information is held on the Crises Control platform.

Cloud Security Principle 4 - Governance framework

The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.

- ✓ Company Board level commitment to and review of information security.
- ✓ Controlled use of administrative privileges for our staff.
- ✓ Maintenance, monitoring, and analysis of security audit logs
- ✓ Transputec has a publicly available [privacy and data protection policy](#) detailing how it handles customer information.
- ✓ Transputec is fully certified to the ISO 9001:2008 Quality Management Standard and to ISO 27001.
- ✓ Our security governance framework is ISO 27001 compliant.

Cloud Security Principle 5 - Operational security

The service provider should have processes and procedures in place to ensure the operational security of the service.

- ✓ Crises Control has the following policies and procedures in place to ensure operational security:
 - A customer vetting policy;
 - A registration and on-boarding policy;
 - A site setup procedure;
 - A deployment procedure;
 - A backup procedure;
 - A monitoring procedure;
 - An escalation of issues procedure;
 - test procedures.
- ✓ In addition we have:
 - A consumer exit procedure;
 - A data destruction procedure;
 - A procedure for the return of the customer data;
 - A change control process.
- ✓ Security checks, management procedures, monitoring procedures, auditing procedures
- ✓ Incident Response and Management procedures.

Cloud Security Principle 6 - Personnel security

Service provider staff should be subject to personnel security screening and security education for their role.

- ✓ Baseline vetting to a minimum of Baseline Personal Security Standard (BPSS).
- ✓ Key operational staffs are SC cleared.
- ✓ All staff are subject to corporate HR policies and procedures
- ✓ All security non-compliance or suspected non-compliance activity is challenged
- ✓ Information security training forms part of the Transputec Academy.
- ✓ Security Skills Assessment and Appropriate Training to fill Gaps.

Cloud Security Principle 7 - Secure development

Services should be designed and developed to identify and mitigate threats to their security.

- ✓ Transputec developers are in possession of the following methodologies and processes to identify and mitigate threats to their security.
- ✓ PRINCE2
- ✓ CRAMM
- ✓ Agile, SCRUM, Sprints,
- ✓ Microsoft Team Foundation Server (TFS)

Cloud Security Principle 8 - Supply chain security

The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement.

- ✓ Our supply chain partners are major international suppliers who fully support all of the 14 security principles that the Crises Control implements. These are:
 - Apple, Microsoft, Blackberry, Google, Coretx and Twilio
- ✓ All supply chain partners are subject to:
 - Financial vetting
 - Reputational vetting
- ✓ As part of our ISO 27001 certified processes.

Cloud Security Principle 9 - Secure consumer management

Consumers should be provided with the tools required to help them securely manage their service.

- ✓ All users have unique user name.
- ✓ Unique password to a minimum secure standard.
- ✓ Application level password policy is enforced.
- ✓ User rights policies.
- ✓ All information assets are managed by authorised users (Consumer administrators).
- ✓ Consumers can manage their accounts through our portal and dashboard.
- ✓ Platform has an option for two keyholders authentication of incidents.
- ✓ Separation of roles within platform into user, keyholder, administrator.
- ✓ Controlled use of administrative privileges.
- ✓ All activities are logged and audited.

Cloud Security Principle 10 - Identity and authentication

Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals.

- ✓ User Roles and Group based security.
- ✓ Crises Control creates the first administrator account and communicates this to a known client representative.
- ✓ Consumers can create additional accounts within the defined user groups only.
- ✓ All accounts have unique complex passwords.
- ✓ All consumer authentication requests and subsequent processing requests are logged and are auditable.
- ✓ Crises Control allows the geographical location of users to be monitored.
- ✓ Crises control app identifies the device from which the user is operating.

Cloud Security Principle 11 - External interface protection

All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them.

- ✓ Resilient internet connectivity is provided via multiple independent ISP circuits delivered into both data centres.
- ✓ Internet connectivity is further protected through the use of a specialist DDoS mitigation service provider.
- ✓ Internet traffic shaping is used to ensure fair-sharing and prevent noisy neighbour (i.e. enforce consumer separation).
- ✓ Our Data Centre has implemented IDS to detect malicious traffic patterns (eg port scans or ICMP flood).
- ✓ Our Data Centre operates managed physical firewalls to restrict the attack surface of customer Solutions.
- ✓ We also use web application firewall (Cloudflare) to protect the website and the portal.
- ✓ Continuous vulnerability assessment and remediation.

Cloud Security Principle 12 - Secure service administration

The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service.

- ✓ All our Data Centre end-user devices used for administration are managed and secured in line with industry best practice.
- ✓ Authorised operations staff manage the platform using corporate end-user devices connecting via secure bastion hosts.
- ✓ We operate ITIL policies and standards.
- ✓ Authorised staff monitor the usage and service.
- ✓ Audit trails monitored.
- ✓ Controlled use of administration rights.
- ✓ Reports on Administrator activity.

Cloud Security Principle 13 - Audit information provision to consumers

Consumers should be provided with the audit records they need to monitor access to their service and the data held within it.

- ✓ Audit trails of messaging activity.
- ✓ Audit trail per incident available.
- ✓ Multiple management reports.
- ✓ Dashboard view of activity.
- ✓ Regular audits.
- ✓ Transputec is fully certified to ISO 9001:2008 Quality Management Systems and ISO 27001:2013 Information Security Management Systems standards. We are also certified to the UK government's Cyber Essentials scheme.

Cloud Security Principle 14 - Secure use of the service by the consumer




Consumers have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected.

- ✓ Monitoring of client activity.
- ✓ Reports, alerts, triggers.
- ✓ Account monitoring and control.
- ✓ Controls outlined in the above principles.
- ✓ Advice provided to consumers on how to work securely with the service.
- ✓ Crises Control helps its consumers to understand security threats and how to be secure in the cloud.

Our partners in Saudi Arabia and UAE, are fully compliant with the provisions of the local laws on data security. Their data centres are hosted locally, minimising latency and comply with all regional laws.

They abide by the following security principles:

- Physical security
 - Cameras – 90 days retention
 - Entrance – Man trap
 - Access Control – 3 factor authentication, all non-employees escorted
 - Nondescript building
 - Physical audit trail
- Perimeter security
 - DDoS Protection
 - Firewall Protection
 - Intrusion Prevention
 - Monitoring & Alerts
 - Network Security
 - Antivirus and Anti-Malware

Data Centers	<ul style="list-style-type: none"> • Full UPS power backup systems and N+1 • Robust HVAC heating, ventilation and CRAC Units • VESDA (Very Early Smoke Detection Apparatus) system across the data center • Control, monitor and record access systems 	
Connectivity	<ul style="list-style-type: none"> • Local ISP Connectivity – UAE (Etisalat/ DU), KSA, Bahrain ... • International Carrier Connectivity – Level 3, Airtel ... • Independent BGP Ring Architecture • Part of UAE-IX with Peering Options 	
Security	<ul style="list-style-type: none"> • Distinct Security Zones • 5 Layer security zones including MAN Trap and Biometric scanning. • 24x7 CCTV Monitoring and Recording with 90 days retention 	

Technology Stack - Security



ISP Security Layer Protection
Rogue IP Quarantine from ISP
Managed DDoS Protection

Inline Perimeter Firewall
Next Generation Inline Firewall with
24x7 Traffic Monitoring



DDoS Protection
On premise DDoS protection + Cloud DDoS
> 1TB DDoS overall mitigation capacity

Dedicated IPS/IDS
Dedicated Intrusion Detection and
Prevention System

businessware
MIDDLE EAST HOSTING SPECIALISTS



Current issue date: 2 June 2020
Expiry date: 31 May 2023
Certificate identity number: 10270904

Original approval(s):
ISO 9001 - 14 July 1999
ISO/IEC 27001 - 23 March 2017

Certificate of Approval

This is to certify that the Management System of:

Transputec Ltd

19 Heather Park Drive, Wembley, London, HA0 1SS, United Kingdom

has been approved by Lloyd's Register to the following standards:

ISO 9001:2015, ISO/IEC 27001:2013

Approval number(s): ISO 9001 - 0004267, ISO/IEC 27001 - 00008809

The scope of this approval is applicable to:

Design, build, integration, implementation and support of business software and hardware solutions, hardware and software product sales, with associated support, provision of fully managed service contracts, including infrastructure platform services, support contracts, contract fulfilment and consultancy services, Statement of Applicability v1.n.

David Derrick

David Derrick

Area Operations Manager UK & Ireland

Issued by: Lloyd's Register Quality Assurance Limited



Lloyd's Register Group Limited, its affiliates and subsidiaries, including Lloyd's Register Quality Assurance Limited (LRQA), and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'Lloyd's Register'. Lloyd's Register assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or otherwise provided, unless that person has agreed a contract with the relevant Lloyd's Register.



CERTIFICATE OF ASSURANCE

Transputec Ltd.

Transputec House, 19 Heather Park Drive, Wembley, Middlesex, HA01SS.

COMPLIES WITH THE REQUIREMENTS OF THE CYBER ESSENTIALS SCHEME

NAME OF ASSESSOR : Simon Ghent
CERTIFICATE NUMBER : IASME-CE-000318
DATE OF CERTIFICATION : 2020/5/13
PROFILE VERSION : February 2017
RE-CERTIFICATION DUE : 2021/5/13
SCOPE : Whole Company

CERTIFICATION MARK



CERTIFICATION BODY



CYBER ESSENTIALS PARTNER



This Certificate certifies that the organisation named was assessed to meeting the Cyber Essentials implementation profile released February 2017 and thus that, at the time of testing, the organisation's ICT defences were assessed to satisfactory against commonly based cyber attack. However, this Certificate does not in any way guarantee that the organisation's defences will remain satisfactory against cyber attack.

Transputec is Cyber Essentials Certified

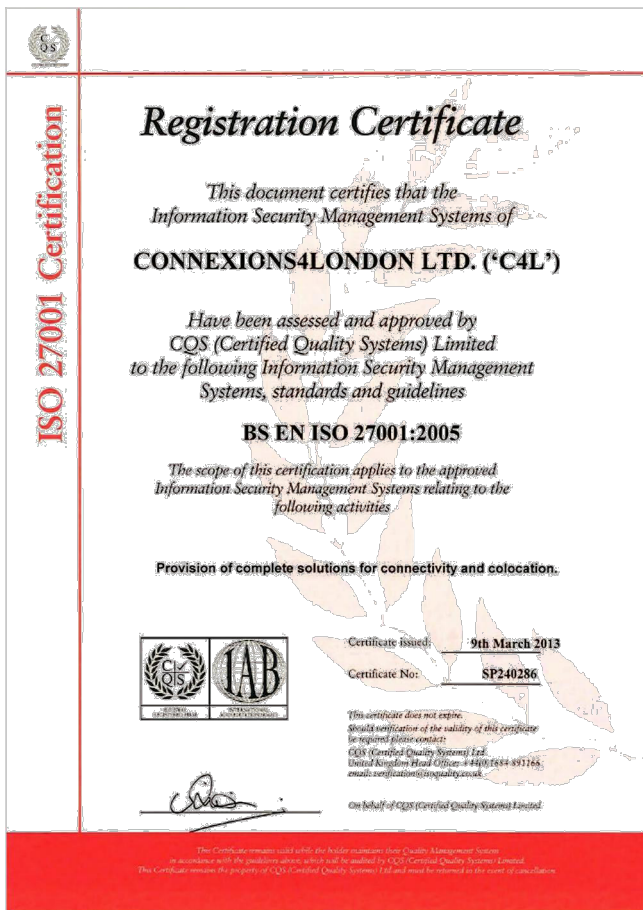


Standard
Consulting
Partner

Transputec is an AWS Select Consulting Partner

Transputec ISO 9001

Transputec ISO/IEC 27001



Coretx ISO 27001

Third-party assurance that Twilio has implemented security best practices on your behalf

ISO 27001

Privacy Shield

SOC 2 for Authy



Please see the embedded white paper for more detail

Twilio Certifications



Twilio ISO/IEC 27001



Twilio hosts it services on Amazon AWS

Certificate



Certificate number: 2015-015

Certified by EY CertifyPoint since: October 1, 2015

Based on certification examination in conformity with defined requirements in ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015, the Information Security Management System as defined and implemented by

Amazon Web Services, Inc.*

and its affiliates (collectively referred to as Amazon Web Services (AWS)) are compliant with the requirements as stated in the standard:

ISO/IEC 27017:2015

Issue date of certificate: November 5, 2019

Re-issue date of certificate: December 8, 2020

Expiration date of certificate: November 7, 2022

Last certification cycle expiration date: November 7, 2019

EY CertifyPoint will, according to the certification agreement dated October 25, 2019, perform surveillance audits and acknowledge the certificate until the expiration date noted above or the expiration of the corresponding ISO/IEC 27001:2013 certification with certificate number [2013-009].

*With regard to the specific requirements for information security as stated in the Statement of Applicability, version 2020.01 dated October 14, 2020, this certification is applicable to (a) the services and their associated assets and locations as described in the scoping section of this certificate, and (b) any affiliates that are responsible for, or that contribute to, the provision of such services and their associated assets and locations.

Designed by:

Jatin Sehgal

REDACTED

J. Sehgal | Director, EY CertifyPoint

08 December 2020 | 3:45:41 PM CET

This certificate is not transferable and remains the property of EY & Young CertifyPoint B.V. located at Antwerp Vredestraat 155, 2083 HP, Amsterdam, the Netherlands. Any dispute relating to this certificate shall be subject to the exclusive jurisdiction of the court in Rotterdam. The content must not be altered and any provision regarding this certificate or certification body quality must refer to the scope and nature of certification and to the conditions of contract. Given the nature and content limitations of sample-based certification assessments, this certificate is not meant to express any form of assurance on the performance of the organization being certified to the relevant ISO standards. The certificate does not grant immunity from any legal/regulatory obligations. All rights reserved. © Copyright

Page 1 of 4

Digital version



Certificate



Certificate number: 2014-014

Certified by EY CertifyPoint since: November 4, 2014

Based on certification examination in conformity with defined requirements in ISO/IEC 17021-1:2015, the Quality Management System as defined and implemented by

Amazon Web Services, Inc.*

and its affiliates (collectively referred to as Amazon Web Services (AWS)) are compliant with the requirements as stated in the standard:

ISO 9001:2015

Issue date of certificate: November 5, 2019

Re-issue date of certificate: December 8, 2020

Expiration date of certificate: November 7, 2022

Last certification expiration date: November 07, 2019

EY CertifyPoint will, according to the certification agreement dated October 25, 2019, perform surveillance audits and acknowledge the certificate until the expiration date noted above.

*This certification is applicable to (a) the services and their associated assets and locations as described in the scoping section of this certificate, and (b) any affiliates that are responsible for, or that contribute to, the provision of such services and their associated assets and locations.

Designed by:

Jatin Sehgal

REDACTED

J. Sehgal | Director, EY CertifyPoint

08 December 2020 | 3:45:41 PM CET

This certificate is not transferable and remains the property of EY & Young CertifyPoint B.V. located at Antwerp Vredestraat 155, 2083 HP, Amsterdam, the Netherlands. Any dispute relating to this certificate shall be subject to the exclusive jurisdiction of the court in Rotterdam. The content must not be altered and any provision regarding this certificate or certification body quality must refer to the scope and nature of certification and to the conditions of contract. Given the nature and content limitations of sample-based certification assessments, this certificate is not meant to express any form of assurance on the performance of the organization being certified to the relevant ISO standards. The certificate does not grant immunity from any legal/regulatory obligations. All rights reserved. © Copyright

Page 1 of 4

Digital version

Twilio hosts its services on Amazon AWS

Twilio hosts its services on Amazon AWS