Vettore Medical
Documento tecnico di sicurezza

Aggiornamento: Apr. 2021
La versione corrente si trova a: http://sicurezza.vettoremedical.it

Disponibilita` del servizio

Non e` previsto di norma nessun downtime per manutenzioni in orari lavorativi.
La SLA e' del 99,95% su base annuale negli orari 7-21 nei giorni da Lunedi a Sabato.
Sono impiegate le tecniche necessarie ad assicurare la disponibilita` continua del servizio 365 giorni all'anno minimizzando le interruzioni, fermo restando il pre-requisito di buon funzionamento della rete globale e della linea internet propria del cliente.

Monitoraggio

L'infrastruttura IT ed i servizi web sono controllati da sistemi di monitoraggio automatici che consentono la manutenzione preventiva di molte delle piu` comuni anomalie di sistema, e che facilitano la gestione degli incidenti in atto.
Gli interventi di risposta ai guasti di natura tecnico-sistemistica possono essere effettuati sia dal personale interno di Vettore Rinascimento, sia da personale incaricato dell'azienda partner "***Laboratori Guglielmo Marconi S.p.A.".***
Il ricorso ad un partner specializzato nel monitoraggio di infrastrutture IT ha l'obiettivo di integrare le risorse interne per garantire il presidio tecnico-sistemistico 365 giorni all'anno e durante tutta la possibile fascia oraria di fruizione dei servizi.

Ridondanza geografica

In caso di guasto ai server, o interruzione di rete o altri incidenti al data-center, le tecnologie di data replication utilizzate permettono il fail-over del sistema verso una struttura completamente separata (in un altra area geografica), in tempi nell'ordine di 10-15 minuti, senza perdita delle ultime operazioni effettuate.
Queste procedure vengono utilizzate e testate regolarmente.

Aggiornamenti del software applicativo

Per la correzione di un difetto al software che venisse eventualmente riscontrato dal cliente, una volta che il problema sia stato corretto internamente dai programmatori, l'aggiornamento al sistema "in produzione" puo` essere eseguito in qualsiasi momento con interruzioni minime di pochi minuti in accordo col cliente.
Le operazioni di aggiornamento applicativo si svolgono con strumenti preposti che minimizzano l'occorrenza di errori operativi al livello di configurazione di sistema.

Salvataggi backup

I salvataggi di backup sono continui, automatici, eseguiti con diversi metodi, e conservati in minimo 3 luoghi diversi (il minimo e' costituito da due dalla lista dei data-center indicati nell'apposito paragrafo, piu` un sistema di solo backup con cifratura presso la sede di Vettore Rinascimento a Bologna.)

In caso di interruzione del servizio per un guasto tecnico al server o al data-center, il ripristino sull'installazione di fail-over richiede nell'ordine dei 10-15 minuti, ed e' senza alcuna perdita di dati inseriti fino all'istante del guasto.
L'archivio "storico" dei backup invece permette il recupero del database ad una qualsiasi data e ora, con una retention di 3 mesi.

I log delle operazioni di backup sono conservati per il periodo di retention, ed il sistema notifica automaticamente il personale addetto nel caso in cui un job di backup non vada a buon fine.
La verifica del recupero dei salvataggi e' effettuata frequentemente nel contesto delle normali operazioni di gestione del servizio.

Oltre alla disponibilità dei dati salvati e storicizzati, con la stessa metodologia attraverso backup dedicati vengono mantenute tutte le configurazioni di sistema, documentate nelle sue parti, al fine di garantire la ricostruzione dell'intero servizio erogato al cliente.

Disponibilita` dei dati

Per rendere fruibile la disponibilità del dato, sono state abilitate le funzioni di esportazione automatiche dei dati, dedicate a figure aziendali del cliente autorizzate attraverso i loro sistemi e comunicate a Vettore Rinascimento; il processo tiene traccia di ogni operazione effettuata.

Collocazione dei server ("Dove sono i dati?")

La rete di Vettore Rinascimento e' distribuita su data-center gestiti da operatori terzi, in varie nazioni europee, il cui elenco -**alla data del documento-** e' il seguente.
L'elenco e' da considerare sempre provvisorio in quanto le strutture utilizzate possono variare per motivi tecnici. La modifica o integrazione di nuovi fornitori terzi, scelti e certificati da Vettore Risarcimento, verrà comunicata al cliente.

Ogni data-center e` una struttura specializzata che ospita attrezzature informatiche su larga scala, con la ridondanza di impianti elettrici, comunicazioni e climatizzazione, la presenza di sistemi antincendio e di sorveglianza, ed il presidio tecnico.

Copie dei dati a scopo di salvataggio (backup) e di sviluppo, sono presenti anche presso la sede operativa Vettore Rinascimento.

Leaseweb Deutschland GmbH *[www.leaseweb.com]* *CED Localita` Frankfurt [DE]* *Certificato: ISO 27001*	*Aruba SpA [www.aruba.it]* *CED Localita` Arezzo [IT]* *Certificato: ISO 27001*	*Hetzner Online GmbH* *[www.hetzner.de/en]* *CED Localita` Falkenstein [DE]* *Certificato: ISO 27001*
OVH [www.ovh.net] *CED Localita` Roubaix [FR]* *Certificato: ISO 27001*	*Scaleway ex Online SAS* *[www.online.net]* *CED Localita` Paris [FR] (c/o ILIAD)* *Certificato: ISO 27001*	*Master Internet Sro* *[www.masterdc.com]* *CED Localita` Brno [CZ]* *Certificato: ISO 27001*
Seflow Snc [www.seflow.net] *CED Localita` Milano [IT]* *Certificato: no*	*Contabo GmbH [www.contabo.com]* *CED Localita` Munich [DE]* *Certificato: no*	*Velia.net Internetdienste GmbH* *[www.velia.net]* *CED Localita` Strasbourg [FR] (Datadock)* *Certificato: no*
Amazon Web Services, Inc. [aws.amazon.com] *CED Localita` varie in UE* *Certificato: ISO 27001*	Netsons Srl [www.netsons.com] *CED Localita` Milano [IT]* *Certificato: ISO 27001*	AltusHost B.V. [www.altushost.com] *CED Localita` Zurigo [CH]* *Headquarter situato ad Amsterdam [NL]* *Certificato: ISO 27001*

Chi ha accesso ai dati

Il personale di Vettore Rinascimento ha la possibilita` di accesso alle informazioni presenti nel gestionale durante lo svolgimento di mansioni come chiamate di supporto tecnico, inserimento dati per conto del cliente o implementazione di modifiche richieste al prodotto, manutenzione del sistema informatico, ecc.
Gli accessi al gestionale da parte del personale autorizzato dell'Assistenza sono effettuati con login strettamente personali e tracciate nei log di sistema.

L'azienda partner "***Laboratori Guglielmo Marconi S.p.A.***" e' certificata ISO 27001, e collabora nel monitoraggio e gestione tecnica da remoto dei sistemi, con il livello di accesso equivalente ai sistemisti interni di Vettore Rinascimento.

Il personale in-loco dei data-center subfornitori, invece, non ha alcun accesso logico ai server ospitati per conto di Vettore Rinascimento, in nessuna fase delle operazioni, in quanto esso interviene esclusivamente su richiesta per semplici operazioni di montaggio / sostituzione fisica di componenti hardware, ma mai invece per interventi di gestione sistemistica.
Le macchine o i dischi che vengono dismessi, e quindi ripresi in carico dai data-center remoti, sono preventivamente sottoposti a cancellazione con metodi di sovrascrittura.

Cifratura

Viene impiegata la cifratura dei dati, "in transito" o "a riposo", inclusi i backup, laddove sussista la concreta possibilita` di furto di supporti fisici, o di intercettazione delle comunicazioni, anche all'interno delle LAN aziendali ed anche nelle trasmissioni tra server.
Il collegamento dalle postazioni di lavoro del cliente e' cifrato con lo standard del web SSL/TLS.

Controlli di accesso logico-applicativo

L'accesso al software gestionale e` soggetto a verifica delle credenziali utente e password.
Il criterio per definire la complessita` delle password e la loro scadenza periodica e` configurabile dal cliente, e presenta per default una impostazione conforme alla normativa.
Il metodo interno di storaggio e autenticazione delle password di accesso del gestionale utilizza le funzioni di ''key derivation''.

Il cliente puo` impostare il blocco degli accessi per-utente da indirizzi rete IP d'origine non riconosciuti.
E` presente un articolato sistema di autorizzazioni dei livelli di accesso in base alla tipologia e mansioni dell'utente.
Gli accessi alla visualizzazione dei dossier sanitari dei pazienti, ed ogni altra informazione correlata come anche fatture o appuntamenti, vengono registrati sui log con data/ora dell'evento, e conservati indefinitamente.

Conservazione dei log

I log relativi all'uso del software gestionale vengono conservati a tempo indeterminato e gli archivi non sono modificabili.

Sicurezza delle postazioni di lavoro e LAN del Cliente

Rimane a cura del cliente il rispetto delle misure di sicurezza concernenti le stazioni di lavoro presso la propria sede (password del PC, bloccaschermo, antivirus, MFA ecc.).
Non gestendo le postazioni di lavoro e le sicurezze implementate a protezione di esse, anche per le reti LAN/WAN del cliente Vettore Rinascimento declina ogni responsabilita` afferente ad esse.

Ambiente di hosting multi-tenant

L'infrastruttura hosting di Vettore Rinascimento prevede la presenza, su ciascun server fisico, di piu` istanze associate a diversi clienti del software gestionale.
La separazione logica tra i servizi erogati a differenti clienti all'interno di un server e` imposta in modo rigoroso, dal sistema operativo del server e dai servizi addizionali, quindi con utenze e autorizzazioni a livello di processo di elaborazione, di filesystem e di database.

Notifica dei data breach

Vettore Rinascimento si impegna a notificare tempestivamente il cliente in caso venisse a conoscenza di una fuoriuscita di dati dolosa o accidentale dal proprio sistema, e di notificarne altrettanto l'Autorita` Garante nei casi previsti dalla legge.

Utilizzo dei dati

Vettore Rinascimento non utilizza i dati in alcun modo al di fuori delle operazioni tecnologiche occorrenti per l'erogazione ed il mantenimento del servizio.
Non si effettuano ricerche sui dati a scopo commerciale, ne` divulgazione a terzi (se non ove venisse richiesto dall'autorita` giudiziaria nei casi previsti dalla legge.)
Non si effetuano trasferimenti di dati, neanche a scopi di backup, presso strutture situate al di fuori dell'UE. Nei casi in cui e` utilizzato un sistema cloud, le nostre risorse virtuali sono comunque mantenute solo nella parte europea.

Figure preposte al trattamento dati personali

Il Responsabile della Protezione Dati (DPO – Data Protection Officer) ai sensi del Regolamento UE 2016/679 "GDPR", e` l'Avv. **Dott. Riccardo De Mare**, del Foro di Bologna.
Il Responsabile del Trattamento e` Vettore Rinascimento Srl, nella persona del legale rappresentante Stefano Matteuzzi.
E` nominato "Amministratore di Sistema" ai sensi della normativa privacy, tutto il personale che si occupa dell'assistenza e gestione del software, nonche` del suo sviluppo, e della gestione tecnica dell'infrastruttura IT, server e cloud.

Per Vettore Rinascimento,
Stefano Matteuzzi

MATTEUZZI STEFANO
Firmato digitalmente da MATTEUZZI STEFANO
Data: 2021.06.08 11:53:49 +02'00'

Certificato

Reg. Numero	11592- L	Valido da	2017-11-10
Primo rilascio	2014-11-19	Ultima modifica	2017-11-10
Scadenza	2020-11-18	Settore	EA: 33

Certificato del Sistema di Gestione per la Qualità

ISO/IEC 27001:2013

Si dichiara che il Sistema di Gestione per la Sicurezza delle Informazioni dell'Organizzazione:

LABORATORI GUGLIELMO MARCONI S.p.A.

è conforme alla norma UNI CEI ISO/IEC 27001:2017 per i seguenti prodotti/servizi:

Monitoraggio e gestione di reti, sistemi e sicurezza ICT.
Progettazione di infrastrutture per reti e telecomunicazioni.

Chief Operating Officer
Giampiero Belcredi

Il mantenimento della certificazione è soggetto a sorveglianza annuale e subordinato al rispetto dei requisiti contrattuali di Kiwa Cermet Italia.
Statement of Applicability (SoA) del 2017-10-25

Il presente certificato è costituito da 1 pagina.

LABORATORI GUGLIELMO MARCONI S.p.A.
Sede Legale
- Via Porrettana, 123 40037 Sasso Marconi Frazione Pontecchio Marconi (BO) Italia

Sedi oggetto di certificazione
- Via Porrettana, 123 40037 Sasso Marconi Frazione Pontecchio Marconi (BO) Italia
- Via Fattori, 6 40033 Casalecchio di Reno (BO) Italia

Kiwa Cermet Italia S.p.A.
Società con socio unico, soggetta all'attività di direzione e coordinamento di Kiwa Italia Holding Srl
Via Cadriano, 23
40057 Granarolo dell'Emilia (BO)
Tel +39.051.459.3.111
Fax +39.051.763.382
E-mail: info@kiwacermet.it
www.kiwacermet.it

SGQ N° 007A SSI N° 006G
SGA N° 010D FSM N° 004I
PRD N° 069B

Certificate

Certificate number: 2013-009

Certified by EY CertifyPoint since: November 18, 2010

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 27001:2013

Issue date of certificate: November 5, 2019
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.

**With regard to the specific requirements for information security as stated in the Statement of Applicability, version 2019.01 dated September 3, 2019, 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.*

J. Sehgal | Director, EY CertifyPoint

Amazon Web Services, Inc.

Scope for certificate 2013-009

The scope of this ISO/IEC 27001:2013 certification is bounded by specified services of Amazon Web Services, Inc. and specified facilities. The Information Security Management System (ISMS) is centrally managed out of Amazon Web Services, Inc. headquarters in Seattle, Washington, United States of America.

The in-scope applications, systems, people, and processes are globally implemented and operated by teams out of an explicit set of facilities that comprise Amazon Web Services, Inc. and are specifically defined in the scope and bounds.

The Amazon Web Services, Inc. ISMS scope includes the services as mentioned on https://aws.amazon.com/compliance/iso-certified/, the locations and AWS Service and Supporting Resources are stated in the following section of this certificate.

The Information Security Management System mentioned in the below scope is restricted as defined in the "ISMS Manual" version 2019.04, signed on October 29, 2019 by the AWS Security Assurance Manager.

Amazon Web Services, Inc.

Scope for certificate 2013-009

Locations in scope:

AWS Services are offered and available across multiple geographic regions around the world. The scope of AWS infrastructure includes corporate headquarters, data center facilities, network and server hardware, and resources which support the datacenter operations.

AWS data centers, which house the hardware supporting the AWS Services listed above. AWS Data centers are located in US East (Northern Virginia), US East (Ohio), US West (Oregon), US West (Northern California), AWS GovCloud (US-East), AWS GovCloud (US-West), Canada (Montréal), EU (Ireland), EU (Frankfurt), EU (London), EU (Paris), EU (Stockholm), EU (Milan),Asia Pacific (Hong Kong), Asia Pacific (Singapore), Asia Pacific (Mumbai), Asia Pacific (Osaka), Asia Pacific (Seoul), Asia Pacific (Sydney), Asia Pacific (Tokyo), and South America (São Paulo) Regions, Middle East (Bahrain), as well as the following AWS Edge Locations in:

- Canberra, Australia
- Melbourne, Australia
- Alexandria, Australia
- Perth, Australia
- São Paulo, Brazil
- Montréal, Canada
- Toronto, Canada
- Vancouver, Canada
- Prague, Czech Republic
- Hong Kong, China
- Copenhagen, Denmark
- London, England
- Manchester, England
- Slough, England
- Stretford, England
- Helsinki, Finland
- Marseille, France
- Paris, France
- Berlin, Germany
- Frankfurt, Germany
- Munich, Germany
- Bengaluru, India
- Chennai, India
- Mumbai, India
- New Delhi, India
- Dublin, Ireland
- Parkwest, Ireland
- Milan, Italy
- Palermo, Italy
- Osaka, Japan
- Tokyo, Japan
- Seoul, Korea
- Kuala Lumpur, Malaysia
- Amsterdam, Netherlands
- Noord Holland, Netherlands
- Sydney, Australia
- Ultimo, Australia
- Vienna, Austria
- Rio de Janeiro, Brazil
- Oslo, Norway
- Manila, Philippines
- Warsaw, Poland
- Singapore
- Cape Town, South Africa
- Johannesburg, South Africa
- Madrid, Spain
- Stockholm, Sweden
- Zurich, Switzerland
- Taipei, Taiwan
- Dubai, United Arab Emirates
- Fujairah, United Arab Emirates
- Arizona, United States
- California, United States
- Colorado, United States
- Florida, United States
- Georgia, United States

Amazon Web Services, Inc.

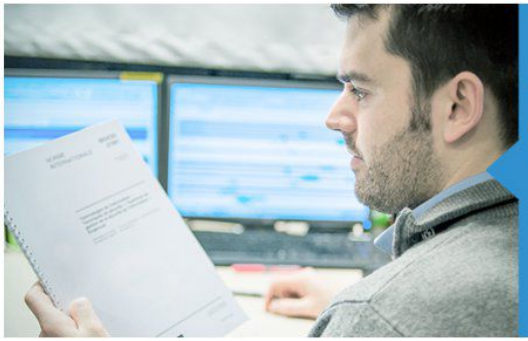
Scope for certificate 2013-009

- Illinois, United States
- Indiana, United States
- Massachusetts, United States
- Minnesota, United States
- Missouri, United States
- Nevada, United States
- New Jersey, United States
- New York, United States
- Ohio, United States
- Oregon, United States
- Pennsylvania, United States
- Texas, United States
- Virginia, United States
- Washington, United States

This scope (edition November 5, 2019) is only valid in connection with certificate 2013-009.

Know how certificato

- Certificazione ISO/IEC 27001
- Certificazione PCI-DSS
- Attestazioni SOC 1 TIPO II E SOC 2 TIPO II
- STAR self-assessment - Cloud Security Alliance
- Il Cloud OVH premiato da VMware
- Best of IT Innovation Award 2014
- Certificazione OpenStack Powered



OVH adotta una strategia di certificazioni e attestazioni volta al riconoscimento globale della conformità delle proprie infrastrutture e servizi agli standard internazionali, che contribuisce ad rafforzare la fiducia tra OVH e i propri clienti e partner.

Certificazione ISO/IEC 27001

ISO 27001 UKAS INFORMATION SECURITY MANAGEMENT KPMG

- OVH ha ottenuto la certificazione ISO/IEC 27001:2013 per il sistema di gestione della sicurezza IT implementato sui propri server dedicati. Per maggiori informazioni, clicca qui.
- L'ISMS per i server dedicati OVH è basato sulla certificazione del datacenter interessato ed è valido per tutti i server ospitati nelle strutture certificate.
- I datacenter conformi sono attualmente quelli di Roubaix (RBX 2,3,5,6,7), Strasburgo, Beauharnois, Singapore e Sydney.

FOX Certification

CERTIFICATE

This is to certify that Quality Management System of

Hetzner Online GmbH
Industriestraße 25
91710 Gunzenhausen

with the scope of

„Data center infrastructure, operations, and server assembly for locations in Nuremberg and Falkenstein"

has been assessed and registered by FOX Certification GmbH and found to be in compliance with the requirements of

ISO/IEC 27001:2013

This verification is subjected to the company maintaining its system to the required standard, which will be monitored by FOX Certification. This certificate is valid for 3 years to satisfactory maintenance of the management system as per the standard.

Statement of Applicability (SoA): V 2.2 (dated 22th of August 2016)
Certificate Expiry: 06th of October 2019
Recertification Date: 06th of October 2019
Certificate: ZN-2016-04

DAkkS
Deutsche Akkreditierungsstelle
D-ZM-18855-01-00

Stuttgart, 11th of October 2016

CEO

MGMT. SYS.
RvA C 466

Certificate

Certificate number: 2014-016
Certified by EY CertifyPoint since:
December 18, 2014

Based on certification examination in conformity with defined requirements in ISO/IEC 17021:2011 and ISO/IEC 27006:2011, the Information Security Management System as defined and implemented by

LeaseWeb*

is compliant with the requirements as stated in the standard:

ISO/IEC 27001:2013

Issue date of certificate: December 18,2014
Expiration date of certificate: December 12, 2017

EY CertifyPoint will, according to the certification agreement (dated November 19, 2014), perform surveillance audits and acknowledges the certificate until the expiration date of the certificate.

**This certificate is applicable for the assets, services and locations of the LeaseWeb companies as described in the scoping section on the back of this certificate, with regard to the specific requirements for information security as stated in Statement of Applicability, version 2.4*

drs. R. Toppen RA
Director EY CertifyPoint

LeaseWeb
Scope for certificate 2014-016

The scope of this ISO/IEC 27001:2013 certification is bounded by the specified services and locations of the independent LeaseWeb companies. The Information Security Management System (ISMS) is centrally managed out of the OCOM Global Services B.V. in Amsterdam, The Netherlands.

The LeaseWeb ISMS scope includes the following services:

- Cloud
- Bare Metal Servers
- Colocation
- Web hosting
- Domains

Locations in scope:

- **LeaseWeb Global Services B.V. / LeaseWeb Netherlands B.V.**
  Luttenbergweg 8
  1101 EC Amsterdam
  Netherlands
- **LeaseWeb USA, Inc.**
  9480 Innovation Drive / Suite 1
  Manassas, VA 20110
  United States of America
- **LeaseWeb Deutschland GmbH**
  Kleyerstrasse 79 / Tor 13
  60326 Frankfurt am Main
  Germany
- **LeaseWeb Asia Pacific PTE. LTD.**
  81 Ubi Avenue 4, #05-03
  408830
  Singapore

The ISMS mentioned in the above scope is restricted as defined in the LeaseWeb ISMS- Scope and Boundaries document as obtained from LeaseWeb's SharePoint site on December 12, 2014.

This Annex (edition: December 18, 2014) is only valid in connection with certificate 2014-016.

BUREAU VERITAS
Certification

ARUBA SPA

Sede Legale e Operativa:
Via San Clemente, 53 - 24036 PONTE SAN PIETRO (BG)

Questo certificato è parte del certificato multisito n. **IT268394**
del **03 aprile 2018** che fa capo a **ARUBA SPA**

Certificato multisito. Il dettaglio dei siti è nell'allegato di questo certificato.

Bureau Veritas Italia Spa certifica che il sistema di gestione dell'organizzazione sopra indicata è stato valutato e giudicato conforme ai requisiti della norma di sistema di gestione seguente

Norma

ISO/IEC 27001:2013

Campo di applicazione

Progettazione, sviluppo ed erogazione di software e servizi di:
- Data Center (Server Dedicati, Server Virtuali, Colocation, Hosting)
- Soluzioni Cloud oriented in modalità IaaS, SaaS e PaaS
- Posta elettronica convenzionale e certificata (PEC)
- Firma digitale e firma qualificata, firma grafometrica e altre soluzioni tecnologiche di firma elettronica avanzata, firma remota, servizi di Certification Authority e personalizzazione di carte a microprocessore (Smart Card)
- Conservazione digitale sostitutiva
- Backup e Disaster Recovery

e relativa assistenza specialistica.
Gestione e manutenzione di server, postazioni di lavoro, reti informatiche e relativi apparati e sistemi di sicurezza logica.
Emissione e gestione di "Identità Digitale" e delle relative credenziali di autenticazione per l'accesso ai servizi "SPID" in qualità di Identity Provider.

DICHIARAZIONE DI APPLICABILITA': Rev. 2.2 del 15/03/2018

Settore/i EA di attività :**33**

Data d'inizio del presente ciclo di certificazione: **10 aprile 2018**

Soggetto al continuo e soddisfacente mantenimento del sistema di gestione questo certificato è valido fino al: **09 aprile 2021**

Data della certificazione originale: **10 aprile 2012**

Certificato N. IT268394/A Rev. N. **1** del: **03 aprile 2018**

ANDREA FILIPPI - Local Technical Manager

Indirizzo dell'organismo di certificazione:
Bureau Veritas Italia S.p.A., Viale Monza, 347, 20126 Milano, Italia

Ulteriori chiarimenti sul campo di applicazione di questo certificato e sui requisiti applicabili della norma del sistema di gestione possono essere ottenuti consultando l'organizzazione.
Per controllare la validità di questo certificato consultare il sito www.bureauveritas.it

ACCREDIA

SGQ	N° 009A	SGE	N° 008N
SGA	N° 008C	SMS	N° 008P
PRD	N° 009B	GHG	N° 008Q
SCR	N° 008F	PSF	N° 009E
PRS	N° 093J	SSI	N° 013Q
PRB	N° 074C		

Membro degli Accordi di Mutuo Riconoscimento EA e IAF
Signatory of EA and IAF mutual Recognition Agreements

4

SECURITY

We provide the highest standards in datacenter security.

HQ: 8 Rue de la Ville-l'Évêque, 75008 Paris sales@iliad-datacenter.fr +33 (0) 1 73 50 29 29 www.iliad-datacenter.fr

DATACENTER SECURITY

Providing first-class security datacenter is our priority. We constantly work to enhance our security protocols and heavily fight all possible threats, ensuring minimum risk to protect your infrastructures and physical assets.

FEATURES

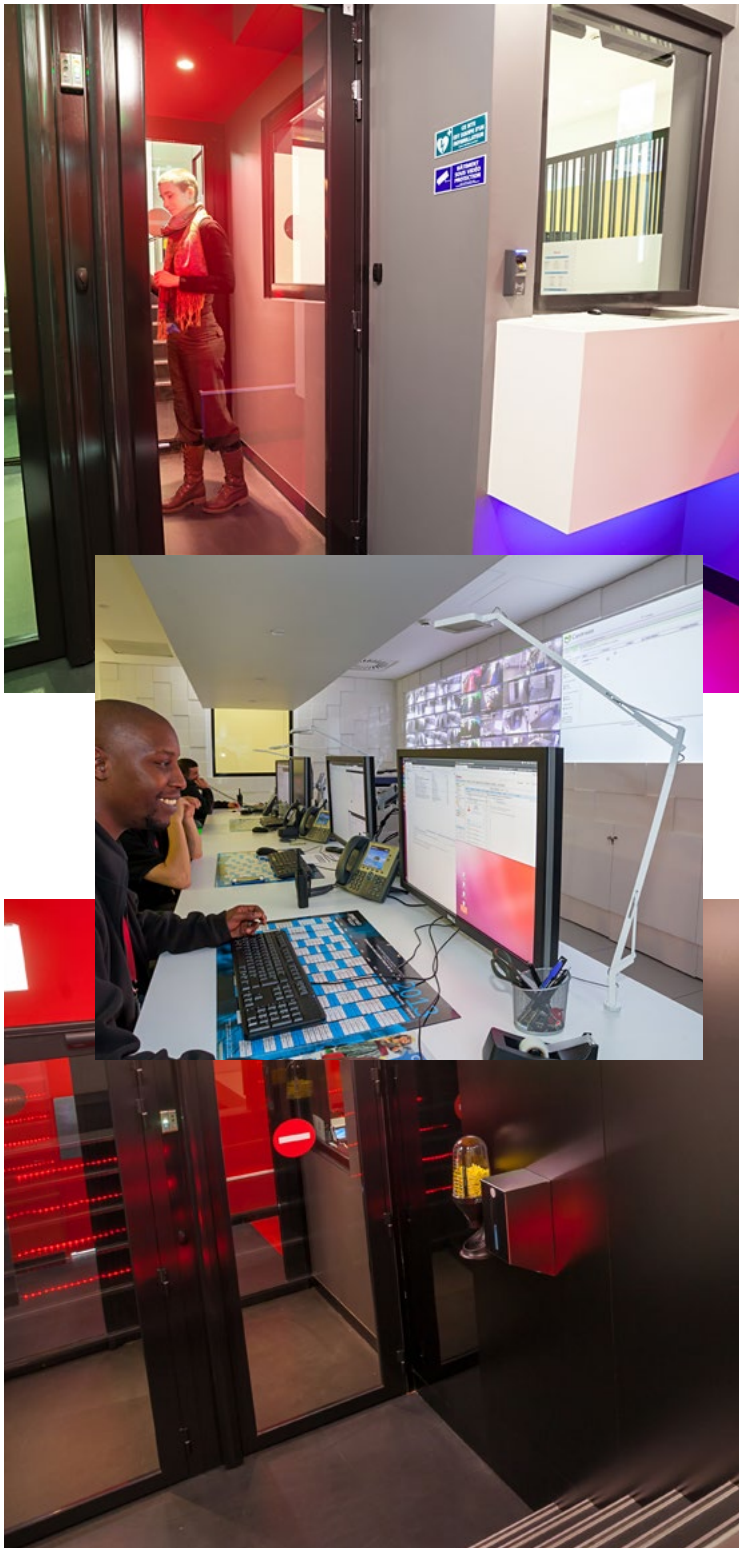
- Multi-stage security containment systems
- Private property with iron fences, gates and restricted access
- Secured car park
- Secured loading docks
- Mantraps and strictly enforced protocols regarding entry access
- Biometrics authentification and RFID Key-card access
- Intrusion detection systems
- Interior managed security zones
- 24/7 internal & external CCTV site coverage
- 60 days online video storage
- Dedicated data halls, suites, and cages to minimize traffic.
- Temperature and humidity monitored, controlled and managed to industry standards
- 24×7 on site security guards
- 24x7 on-site NOC services
- 24x7x365 on-site technical team
- Pre-action, zoned dry-pipe sprinkler (water mist) systems for fire suppression
- Natural risk free locations
- WiFi network access and cell phone repeaters/boosters through-out the facility

CERTIFICATIONS

- pci-DSS*
- HDS*
- ISO 27001*

**2017*

Enjoy peace of mind knowing your critical information systems are secure and protected. We take extreme precautions to safeguard your hardware and data. Only people you authorize can access to your infrastructure. Our security systems are tested continuously to ensure complete protection of the data center and of our customer infrastructures.



Certificate no.: TCB 18/07/127243

tayllorcox.com
ensure your certification

Certificate

Information Security Management System

Master Internet, s.r.o.

Identification No.: 262 77 557
Jiráskova 225/21, 602 00 Brno, Czech Republic
datacentre: Kodaňská 46, 101 00 Praha 10, Czech Republic
Cejl 20, 602 00 Brno, Czech Republic
administration: Purkyňova 35e, 602 00 Brno, Czech Republic

has been examined and found in conformity with requirements of the standard

ISO/IEC 27001:2013

for the following range of activities:

The operation of data centers; hosting and cloud services; software development.

Date of the initial certification:	20.8.2015
Date of the certification:	29.6.2018
This certificate is valid until:	28.6.2021

Company director

THINK-TANK IN BIRMINGHAM

Place and date of issue of the certificate: Prague, 20.7.2018
This certificate is valid with the Statement of Applicability from 31.1.2017.

S 3210

The certificate was issued by TAYLLORCOX s.r.o.
Na Florenci 1055/35, Staré Město - Praha 1, CZ 110 00, info@tayllorcox.com, www.tcox.cz
To check this certificate validity please call the phone number: +420 222 553 101
Member of: TAYLLORCOX UK Ltd., 75 King William St., EC4N, London, United Kingdom, info@tayllorcox.com