Maggioli Informatica

è un marchio **Maggioli Spa**

Santarcangelo di Romagna, 14/12/2020

DICHIARAZIONE DI CONFORMITA SERVIZI CLOUD MAGGIOLI IN TEMA DI MISURE MINIME DI SICUREZZA (Circ. Agid 2/2017)

Gentile Cliente,

con la presente si informa che i servizi Cloud di Maggioli S.p.a. erogati dai propri Datacenter sono conformi alle indicazioni della Circolare Agid n.2/2017 del 18 aprile 2017 in relazione alle «*Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015*)».
I nostri servizi Cloud Hosting/IaasS/PaaS sono sottoposti a specifiche e rigorose certificazioni e controlli inerenti la sicurezza dei dati quali ISO27001 (di cui riportiamo il certificato) e ne rispettano le direttive Agid sino a permettere a Maggioli Spa lo status di conservatore accreditato Agid (http://www.agid.gov.it/agenda-digitale/pubblica-amministrazione/conservazione/elenco-conservatori-attivi)
Poiché per precisione la circolare n.2/2017 riporta punti di diversa competenza e dominio (postazioni e/o risorse locali, dominio di tipo applicativo ecc..) elenchiamo di seguito quelli correlati a servizi Cloud Hosting/IaasS/PaaS oggetto della presente dichiarazione di conformità.

Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	ABSC 1.1.1
Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	ABSC 1.1.3
Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	ABSC 1.3.1
Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	ABSC 2.3.1
Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	ABSC 2.3.3
Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	ABSC 3.1.1
Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	ABSC 3.2.1

Maggioli Informatica
via Bornaccino, 101
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 621153
informatica@maggioli.it
www.maggioli.it

Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	ABSC 3.2.2
Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	ABSC 3.4.1
Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	ABSC 4.1.1
Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	ABSC 4.4.1
Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	ABSC 4.5.1
Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio	ABSC 4.7.1
Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	ABSC 4.7.2
Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	ABSC 4.8.1
Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	ABSC 4.8.2
Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	ABSC 5.1.1
Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	ABSC 5.1.2
Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	ABSC 5.2.1
Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	ABSC 5.5.1
Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	ABSC 5.7.3
Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	ABSC 5.7.3
Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le	ABSC 5.10.3

Maggioli Informatica
via Bornaccino, 101
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 621153
informatica@maggioli.it
www.maggioli.it

situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	
Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	ABSC 5.11.1
Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	ABSC 8.1.3
Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	ABSC 10.1.1
Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	ABSC 10.1.2
Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	ABSC 10.1.3
Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	ABSC 10.2.1
Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	ABSC 10.3.1
Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	ABSC 10.4.1

Maggioli Informatica

è un marchio **Maggioli Spa**

AntiMalware, Data Retention e Manutenzione Programmata.

In aggiunta alla risoluzione delle specifiche AGID sopra indicate il sistema di gestione a norme ISO27001 applicato nella gestione dei DataCenter Maggioli definisce e garantisce i seguenti parametri tecnico/operativi:

- A livello perimetrale per i servizi contenuti è implementata una rete firewall di ultima generazione Fortinet che implementa funzionalità antimalware, antispam, DDOS con capacità di auto-aggiornamento delle firme malware in base oraria.
- Sempre a livello globale, tramite tecnologia di backup virtuale VMWare, è implementato il sistema di backup con una ciclicità che, in determinazione delle specificità applicative e progettuali del servizio, può variare da minimo di 30 giorni ad un massimo di 180 definendo così automaticamente su questi valori anche i parametri minimi e massimi di data-retention.
- Le procedure ISO27001 implementate definiscono infine le seguenti tipologie di attività di manutenzione programmata:
  - Controlli antimalware e backup -> Settimanali
  - Controlli estesi delle piattaforme HW e networking -> Mensili

Cordiali Saluti

Maggioli Informatica
Responsabile Sistemi
Oscar Bevoni

Maggioli Informatica
via Bornaccino, 101
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 621153
informatica@maggioli.it
www.maggioli.it

Maggioli Informatica

è un marchio **Maggioli Spa**

DNV·GL

MANAGEMENT SYSTEM CERTIFICATE

Certificato No./Certificate No.:
276910-2018-AIS-ITA-ACCREDIA

Data prima emissione/Initial date:
09 marzo 2010
Data precedente OdC/
Previous CB date

Validità/Valid:
08 marzo 2019 - 08 marzo 2022

Si certifica che il sistema di gestione di/This is to certify that the management system of

MAGGIOLI S.p.A.

Sede Legale: Via del Carpino, 8 - 47822 Santarcangelo di Romagna (RN) – Italy
e i siti come elencati nell'Appendix che accompagna questo certificato /
and the sites as mentioned in the appendix accompanying this certificate

È conforme ai requisiti della norma per il Sistema di Gestione/
Has been found to conform to the Management System standard:

ISO/IEC 27001:2013

Questa certificazione è valida
per il seguente campo applicativo:

Analisi, progettazione, sviluppo, manutenzione e assistenza di software per la Pubblica Amministrazione e Aziende erogato anche in modalità SaaS. Erogazione di servizi applicativi in ambito IT come System integrator di prodotti propri e di terze parti. Erogazione di servizi di inserimento dati, anche presso la sede del cliente, stampa, rendicontazione, invio in multicanalità e supporto alla riscossione delle sanzioni amministrative degli atti elevati della Polizia Locale o da altri uffici della Pubblica Amministrazione. Erogazione di servizi di housing, hosting, IaaS, PaaS, Disaster Recovery e Cloud Computing in accordo alle linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2014. Erogazione di servizi di conservazione a norma di documenti informatici

(EA: 35, 33)

In accordo alla Dichiarazione di Applicabilità del 28 giugno 2019, Rev. 5

This certificate is valid
for the following scope:

Analysis, design, development, maintenance and assistance of software for the Public Administration and Companies provided also in SaaS mode. Provision of IT application services as a System integrator of proprietary and third parties products. Provision of data entry services, even at customer sites, printing, reporting, multi-channel mailing and support for the collection of the administrative sanctions of the administrative acts of Local Police and other offices of the Public Administration. Provision of housing, hosting, IaaS, PaaS, Disaster Recovery and Cloud Computing according to ISO/IEC 27017:2015 and ISO/IEC 27018:2014 Guidelines. Provision of digital preservation services for IT documents

(EA: 35, 33)

In accordance with the Statement of Applicability of 28 june 2019, Rev. 5

Luogo e Data/Place and date:
Vimercate (MB), 02 agosto 2019

ACCREDIA

Per l'Organismo di Certificazione/
For the Certification Body

~~Zeno Beltrami~~
Management Representative

La validità del presente Certificato è subordinata al rispetto delle condizioni contenute nel Contratto di Certificazione/
Lack of fulfilment of conditions as set out in the Certification Agreement may render this Certificate invalid.
DNV GL Business Assurance Italia S.r.l. Via Energy Park, 14, 20871 Vimercate (MB), Italy. Tel: 039 68 99 905. www.dnvgl.it/assurance

Maggioli Informatica
via Bornaccino, 101
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 621153
informatica@maggioli.it
www.maggioli.it