Nuvyta Srl
Via Mozart, 47
20093 Cologno Monzese (MI)
T. +39 02 2217 9862
F. +39 02 2117 9863
info@nuvyta.com
www.nuvyta.com
P.IVA 10223560961

INFORMATION SECURITY CONTROLS FOR CLOUD SERVICES AND FOR PROTECTING PERSONAL DATA IN THE CLOUD

INTEGRATED MANAGEMENT SYSTEM

Nuvyta è un'azienda, fondata nel Febbraio 2018 da un Gruppo di persone con pluriennale esperienza in ambito IT clinico. Nuvyta nasce dall'idea che la tecnologia può fare la differenza tanto quanto la fanno le persone.

Le conoscenze tecniche e le competenze in ambito sanitario del team, si pensa possano cambiare la difficile relazione tra clinici e software.

Obiettivo primario dell'Organizzazione è la realizzazione di una **Piattaforma di collaborazione clinica** dotata di un ambiente di configurazione e programmazione web visuale e basata sui principi di interoperabilità, sicurezza e scalabilità. Si tratta di una piattaforma cloud con cui il cliente può personalizzare i processi clinici senza dover sviluppare codice e collaborare real time con pazienti e colleghi.

La Direzione **si impegna a** raggiungere i seguenti obiettivi:

Obiettivi ISO 27017

- Definire quali siano i requisiti minimi di sicurezza applicabili alla progettazione e all'implementazione dei servizi sul cloud (il minimo tutelabile)
- Definire i rischi derivanti da utilizzatori non autorizzati (da inserire nell'analisi dei rischi);
- Definire i criteri di isolamento degli ambienti multi-tenancy e virtualizzazione;
- È previsto l'accesso agli assets del cliente conservati in Cloud da parte dello staff di Nuvyta;
- Attuare Procedure di controllo degli accessi e forti vincoli di autenticazione per gli amministratori di sistema dei servizi in cloud;
- Che vengano comunicati ai clienti i change management sugli ambienti cloud;
- Garantire sicurezza della virtualizzazione degli ambienti;
- Accesso e protezione dei dati dei clienti sul cloud
- Accesso e protezione dei dati dei clienti del servizio cloud;
- Gestione del ciclo di vita degli account del cliente;
- Comunicazione di violazioni e condivisione delle informazioni per agevolare le indagini forensi;

Document Information

DocCode	*Q_P_007 - ITA*			Version	1.0
Title	*Q_P_CloudComputing_ISO27017&ISO27018*			Created	10/01/2023
				Modified	10/01/2023
Author	Chiara Savino	Reviewer	Vania Manzelli	Approver	Alice Magni

Nuvyta Srl
Via Mozart, 47
20093 Cologno Monzese (MI)
T. +39 02 2217 9862
F. +39 02 2117 9863
info@nuvyta.com
www.nuvyta.com
P.IVA 10223560961

- In fase di setup dell'ambiente cloud, è necessario garantire la coerenza tra reti virtuali e fisiche.

Obiettivi ISO 27018

- Stabilire contratti chiari, completi e in conformità alla legge
- Definizione lineare di ruoli e responsabilità per i servizi cloud erogati (es. Saas, Paas etc)

La Direzione **assicura** quanto sotto:

Garanzia al cliente in conformità alla ISO 27017

- Le informazioni contenute nell'ambiente cloud possono essere soggette a accesso e gestione da parte del gestore del cloud (Nuvyta)
- Che gli assets possono essere conservati nell'ambiente cloud (Ad esempio programmi applicativi)
- Che i processi possono essere svolti su cloud virtuali con pluralità di utenti mantenendo la singolarità di accesso ai dati
- Quali sono gli utilizzatori dei servizi e il contesto nel quale i servizi in cloud sono utilizzati
- Gli amministratori del servizio cloud sono coloro che hanno accessi privilegiati nel cloud service customer;
- La localizzazione geografica dell'organizzazione del cloud service provider e dei paesi in cui Nuvyta archivia i dati del cloud service customer (anche se solo temporaneamente).

In qualità di Cloud Service Customer, Nuvyta **assicura**:

- Per ogni servizio cloud acquistato/utilizzato, l'identificazione delle modalità di accesso al cloud;
- Che l'accesso ai servizi cloud utilizzati da Nuvyta, avvenga tramite autenticazione MFA;
- La verifica della compatibilità dei software utilizzati in azienda nei confronti dei servizi cloud acquistati e la conformità delle licenze d'uso installate sul Cloud Service Provider;
- Che i servizi cloud utilizzati prevedano che le informazioni relative alla gestione delle chiavi crittografate vengano comunicate in termini di procedure da adottare;
- la scelta del Cloud Service Provider a valle di un processo di qualifica del fornitore, che si basi sulla verifica di:
    - rispetto di adeguati standard di sicurezza;
    - conformità dei requisiti nella gestione del logging;
    - corretta gestione degli incidenti in merito alla sicurezza delle informazioni;
    - garanzia su normative e leggi del territorio presso cui ha sede il cliente;
    - abbia politiche e procedure per lo smaltimento e il riutilizzo di risorse;
    - la conformità ai controlli crittografici proposti;
    - una procedura per i fornitori che si applica anche ai CSP, che prevede la raccolta di certificazioni che attestano la sicurezza informatica

Garanzie al cliente in conformità alla ISO 27018

- Le informazioni relative alle policy di sicurezza delle informazioni vengono potenziate includendo una dichiarazione di supporto e dedizione per raggiungere il pieno rispetto delle leggi in vigore in materia di PII e dei vincoli contrattuali presenti tra il l'addetto competente PII del cloud e i clienti.
- Negli accordi contrattuali vengono definiti chiaramente le responsabilità tra l'addetto PII del cloud, i sub appaltatori e i clienti dei servizi in cloud, considerando quale siano le specifiche tipologie di servizio (IaaS, SaaS, PaaS etc).

Document Information

DocCode	*Q_P_007 - ITA*			Version	1.0
Title	*Q_P_CloudComputing_ISO27017&ISO27018*			Created	10/01/2023
				Modified	10/01/2023
Author	Chiara Savino	Reviewer	Vania Manzelli	Approver	Alice Magni

Nuvyta Srl
Via Mozart, 47
20093 Cologno Monzese (MI)
T. +39 02 2217 9862
F. +39 02 2117 9863
info@nuvyta.com
www.nuvyta.com
P.IVA 10223560961

- Utilizzo di servizi PAAS che non prevedano, per l'archiviazione dei dati, una riallocazione per nuovi clienti di Storage dismessi su altri clienti a meno di garanzia di chiavi di cifratura differenziate per cliente.

Tale politica si integra alla Politica della qualità (Q_P_QualityPolicy) e la Politica per la sicurezza delle informazioni (Q_P_SecurityQualityPolicy) come politiche cardini del Sistema di Gestione integrato.