1. INTRODUZIONE

Il cloud computing offre molti potenziali benefici, tra cui scalabilità, elasticità, alte prestazioni, minori carichi per la sua amministrazione insieme a efficienza in termini di costi, agilità, flessibilità, tempi di immissione sul mercato più rapidi e nuove opportunità di innovazione.
Comprendere, gestire e controllare i rischi che riguardano principalmente la riservatezza, la sicurezza e la resilienza legati all'adozione e/o all'erogazione di servizi in cloud è fondamentale per garantire una corretta gestione della sicurezza delle informazioni.

2. SCOPO E CAMPO DI APPLICAZIONE

Il presente documento definisce le politiche aziendali specifiche, parti integranti della politica generale del SGI definita dalla Direzione di METEDA, relativamente al servizio Cloud, per la protezione dei dati globali, inclusi i dati personali applicando le best practices definite dagli standard ISO 27017 e ISO 27018.
Lo scopo di questa politica pertanto è descrivere i principi generali di sicurezza nell'ambito dei servizi in cloud che METEDA ha fatto propri, al fine di garantire una sicurezza delle informazioni, conservate e/o gestite su piattaforme in cloud pubblici, di livello almeno pari ai principi generali espressi nella sua politica generale di sicurezza e, in presenza di dati personali, conformi alla normativa vigente.

3. PERIMETRO ORGANIZZATIVO

La presente policy si applica a tutto il personale dipendente di METEDA e a tutti i soggetti che collaborano con la stessa.
La policy si applica inoltre a tutti i processi più in generale e a tutte le risorse coinvolte nella gestione delle informazioni trattate dalla società.
Nel documento, i termini "fornitore di servizi cloud" o "CSP", acquistano una duplice valenza a seconda del contesto. Quando la policy verrà applicata a servizi di cui METEDA è cliente, con i suddetti termini ci si riferirà al fornitore di tali servizi. Quando verrà applicata a servizi erogati da METEDA, ci si riferirà all'azienda.

4. TERMINI E DEFINIZIONI

Asset o Bene – Qualsiasi risorsa che abbia un valore per l'organizzazione, sia essa materiale o immateriale (es. beni fisici, software, informazioni e dati, …).

Cloud – Un insieme di servizi ICT accessibili on-demand e in modalità self-service tramite tecnologie Internet, basati su risorse condivise, caratterizzati da rapida scalabilità e dalla misurabilità puntuale dei livelli di performance, in modo da poter essere pagati in base al consumo.

Cloud Privato– Piattaforma basata su Cloud gestita internamente per erogare servizi e non aperta alla disponibilità di soggetti terzi.

Cloud Pubblico – Piattaforma basata su Cloud che eroga servizi a più soggetti non connessi tra di loro.

Cloud Ibrido – Soluzione tecnologica che prevede l'impiego combinato di Cloud Pubblico e Cloud Privato.

CSP – (Cloud Service Provider) Un'entità (privata o pubblica) che fornisce piattaforme, infrastrutture, applicazioni, servizi di sicurezza o di archiviazione basati su cloud a un'altra entità/organizzazione solitamente a pagamento.

Disponibilità – Proprietà per la quale le informazioni sono rese accessibili ed utilizzabili su richiesta di un'entità autorizzata (ISO/IEC 13335-1:2004).

Hardening – Insieme di azioni atte ad analizzare le funzionalità di un sistema operativo/applicazione al fine di individuare la configurazione ottima che permetta di innalzare il livello di sicurezza e ridurre il rischio residuo connesso alle debolezze dei sistemi.

IaaS – (Infrastructure-as-a-Service) Infrastruttura erogata in modalità di servizio. Risorse hardware virtualizzate vengono messe a disposizione, affinché l'utilizzatore possa creare e gestire, secondo le proprie esigenze, una propria infrastruttura sul cloud senza preoccuparsi di dove siano allocate le risorse

Integrità – Proprietà per la quale l'accuratezza e la completezza degli asset è salvaguardata (ISO/IEC 13335-1:2004).

Log - Il log è un sistema di registrazione di avvenimenti significativi. I file che contengono queste annotazioni sono detti file di log e potrebbero essere identificati anche come i file delle registrazioni, per cui il log è non è altro che un registro.

Responsabile del Trattamento - la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento; Riservatezza – Proprietà per la quale le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati (ISO/IEC 13335-1:2004).

Snapshot – Copia dello stato di una macchina virtuale in un determinato momento.

Titolare del Trattamento - la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

VM – Le macchine virtuali sono software, creati all'interno di un ambiente digitale, che offrono le stesse funzionalità dei computer fisici.

5. CONTESTO REGOLATORIO DI RIFERIMENTO

- ISO 27001:2013 – Sistemi di gestione per la sicurezza delle informazioni – Requisiti
- ISO 27017:2015 – Codice di pratica per i controlli di sicurezza delle informazioni basati su ISO / IEC 27002 per i servizi cloud
- ISO 27018:2019 – Codice di pratica per la protezione delle informazioni personali (PII) in cloud pubblici che agiscono come processori PII
- GDPR Reg. UE 679/2016 e legislazione nazionale

6. POLITICA DI SICUREZZA DI GESTIONE SERVIZIO CLOUD

METEDA eroga servizi di cloud computing in modalità SaaS (Software-as-a-Service) in quanto i servizi all'utente finale sono erogati tramite applicazioni basate sul Web. Il modello SaaS è un metodo per la distribuzione di applicazioni software tramite Internet, dove i provider di servizi cloud ospitano e gestiscono tali applicazioni software per consentire l'uso delle stesse da tutti i dispositivi.

METEDA, nell'utilizzare la infrastruttura IAAS a supporto dei propri processi, acquisisce il ruolo di Cloud Service Customer.
Il Cloud METEDA offre all'utente finale le seguenti tipologie di servizi a valore aggiunto:

- scambio limitato di informazioni tra l'applicazione, installata volontariamente dall'Utente/Interessato sul proprio device (smartphone, tablet e similari) e l'infrastruttura IT della struttura sanitaria/Professionista di riferimento, al solo fine di rendere operativa la messaggistica asincrona bidirezionale tra il singolo paziente e il proprio medico curante, Titolare autonomo del trattamento,
- scambio limitato di informazioni tra l'applicazione, installata volontariamente dall'Utente/Interessato sul proprio device (smartphone, tablet e similari) e l'infrastruttura IT allestita ad hoc da METEDA, con architettura CLOUD, per l'utilizzo di prodotti di soggetti terzi.

Nell'ambito dell'erogazione e/o gestione di servizi cloud METEDA prende in considerazione i requisiti di seguito descritti.

- Gestione del Cloud: lo spostamento di dati nel cloud può richiedere un riallineamento significativo di ruoli e responsabilità all'interno dell'organizzazione e/o nei confronti dei suoi fornitori. Per questo motivo è necessario definire puntualmente i ruoli tanto relativamente all'erogazione del servizio quanto alla gestione delle relazioni con i fornitori di servizi cloud.
  Il personale con responsabilità dirette relativamente ai servizi su cloud pubblico è formato sulle tecnologie cloud, sulle disposizioni in materia di trattamento di dati personali.
- Virtualizzazione: Nel cloud computing, la maggior parte dei controlli di separazione logica non sono fisici (ovvero server separati). La separazione viene forzata attraverso l'utilizzo di apparati virtuali e la segmentazione e l'integrità dei dati viene garantita attraverso controlli logici. METEDA opera per garantire, nell'ambiente virtuale, un livello di sicurezza della separazione dei sistemi almeno analogo a quello degli ambienti fisici.
- Separazione degli ambienti: nel Cloud Pubblico le infrastrutture fisiche sono condivise con altri utenti e con il gestore della piattaforma stessa. METEDA garantisce una corretta separazione delle diverse realtà logiche.
- Gestione delle identità digitali: la gestione delle identità digitali è una componente essenziale per garantire la sicurezza dei dati nel cloud computing. METEDA garantisce una loro corretta gestione durante tutto il ciclo.
- Gestione dei Log: METEDA dispone delle necessarie informazioni relative ai log di monitoraggio e garantisce l'accesso ai soli utenti autorizzati.
- Sicurezza delle applicazioni Web: il cloud è, in genere, un ambiente aperto. Questo aspetto aumenta significativamente l'esposizione agli attacchi. Per questa ragione METEDA sottopone a controlli suppletivi le applicazioni web che si interfacciano con ambienti Cloud pubblici.
- Disaster Recovery: sui dati conservati in Cloud, METEDA effettua verifiche puntuali per garantire la loro disponibilità anche in caso di disastro.
- Indagini informatiche: le autorità competenti possono richiedere l'accesso ad informazioni specifiche nell'ambito di attività d'indagine. Come per i dati archiviati internamente, è necessario avere delle procedure condivise con il fornitore quando i dati sono archiviati da un CSP.
- Requisiti contrattuali: prima di trasferire i dati a terzi METEDA effettua un'analisi del CSP e adotta specifiche clausole contrattuali.
- Trattamento dei dati personali: i ruoli e le responsabilità nell'ambito del trattamento dei dati personali conservati su un cloud pubblico sono chiaramente definiti.

Nel seguito vengono descritte le principali attività necessarie per recepire i requisiti sopra riportati.

7. GESTIONE DEL CLOUD

7.1 RUOLI E RESPONSABILITA' PER LA SICUREZZA DELLE INFORMAZIONI

Per consentire un'efficace attività di gestione dei servizi cloud METEDA assicura che:

- Il personale con responsabilità dirette relativamente ai servizi su cloud è formato sulle tecnologie cloud, sulle disposizioni in materia di trattamento di dati personali.
- Nel caso di acquisizione di servizi cloud sul mercato, sulla gestione dei fornitori sono definiti e documentati i diversi ruoli e responsabilità per il personale responsabile della gestione del servizio cloud, sono formalizzati Quality Technical agreement per assicurare il livello del servizio erogato, sono inoltre sottoscritti NDA a garanzia della sicurezza e riservatezza delle informazioni.
- Tali ruoli sono condivisi anche con i clienti quando METEDA opera in qualità di CSP. In tal caso è definito e condiviso con i clienti un processo di escalation verso il gruppo responsabile della gestione dei servizi cloud.

L'identità del Responsabile del trattamento, è la seguente:
METEDA SRL
indirizzo: Via Antonio Bosio, 2 Int.10 - 00161 Roma (RM)
Sede Amm. ed Operativa: Via Silvio Pellico, 4 - 63074 San Benedetto del Tronto (AP)
contatti: e-mail info@meteda.it Telefono: +39 0735 783021 Fax: +39 0735 83887

Il controllo della gestione in sicurezza dell'infrastruttura Cloud è assicurato da un team di tecnici specialisti composto da risorse interne all'organizzazione METEDA e da fornitori esterni qualificati.
Per informazioni di dettaglio:

- Responsabile Sicurezza Cloud - assistenza@meteda.it
- DPO - privacy@meteda.it

7.2 SEDE GEOGRAFICA TRATTAMENTO DEI DATI

I servizi cloud di METEDA sono hostati su VM Azure di Microsoft, dotate dei più alti standard di sicurezza disponibili sul mercato e residenti in server farm geograficamente distribuite nel rispetto delle policy di business del prodotto e delle normative vigenti .
Per informazioni di dettaglio:

- Responsabile Sicurezza Cloud - assistenza@meteda.it

7.3 GESTIONE DEGLI ASSET E CLASSIFICAZIONE DELLE INFORMAZIONI

L'accesso agli asset del cliente avviene in relazione alle disposizioni contrattuali ed in conformità con le disposizioni legislative.

A tutela dei diritti degli interessati i cui dati sono oggetto del trattamento, METEDA si impegna ad informare costantemente i propri clienti su politiche, pratiche e tecnologie di sicurezza dei dati e di privacy applicate.
Questi impegni includono:

- Accesso e proprietà: il cliente conserva il pieno controllo dei propri contenuti. La proprietà dei dati rimane al cliente.
- Divulgazione dei contenuti dei clienti: METEDA non divulga i contenuti del cliente se non richiesto dalla legislazione vigente o da ordinanze vincolanti emesse da un'autorità statale;
- Controlli di Sicurezza: METEDA adotta politiche, standard e linee guida su privacy e protezione dei dati per raggiungere il più alto livello di sicurezza e confidenzialità.

7.4 GESTIONE ACCESSI UTENTE

L'accesso ai Servizi cloud da parte dell'utente avviene attraverso un processo di registrazione e/o comunque di download volontaria dell'app associata al servizio.

I dati trattati sono quelli relativi ai dati identificativi degli utenti ed a seconda del servizio potrebbe essere prevista la gestione di dati personali relativi alla salute dell'interessato, siano essi in transito o anche con funzione di repository.

La Cancellazione della registrazione avviene su richiesta dell'interessato, nel rispetto del GDPR secondo le modalità descritte nell'informativa privacy.
L'interessato, nel caso di accesso al servizio mediante il download di una app, può utilizzare la procedura di disinstallazione standard a sua disposizione tramite il dispositivo mobile.

8. VIRTUALIZZAZIONE SUI SISTEMI ACQUISITI SUL MERCATO

La maggior parte dei controlli di separazione logica non sono fisici (ovvero server separati). La separazione viene forzata attraverso l'utilizzo di apparati virtuali e la segmentazione e l'integrità dei dati viene garantita attraverso controlli logici. METEDA opera per garantire, nell'ambiente virtuale, un livello di sicurezza della separazione dei sistemi almeno analogo a quello degli ambienti fisici.

Per consentire un'efficace protezione dei sistemi virtuali:

- in fase di valutazione del fornitore sono valutate le politiche di sicurezza adottate prestando particolare attenzione all'adozione di standard e best practice riconosciuti. Le politiche, a titolo esemplificativo, contemplano i seguenti aspetti:
    - disabilitazione (o rimozione) di tutte le interfacce, porte, servizi e dispositivi non strettamente necessari;
    - configurazione con principi di sicurezza delle informazioni di tutte le interfacce di rete virtuali e le aree di archiviazione;
    - limiti sull'utilizzo delle risorse della VM;
    - hardening (adozione di politiche di sicurezza) di tutti i sistemi operativi e delle applicazioni in esecuzione all'interno della macchina virtuale;
    - validazione dell'integrità delle operazioni di gestione delle chiavi crittografiche;
- Il CSP adotta controlli per garantire che vengano acquisiti solo gli snapshot previsti e autorizzati e che il livello di classificazione, posizione di archiviazione e crittografia che gli viene assegnato sia in linea con la sensibilità dei dati trattati
- assicura inoltre che i seguenti controlli siano applicati:
    - accesso agli access log amministrativi dell'hypervisor;
    - registrazione di tutti i log dell'hypervisor
- METEDA deve supportare l'utilizzo di VM fornite dal cliente e dallo stesso considerate affidabili
- METEDA, identifica l'elenco completo dei suoi fornitori coinvolti nella gestione del cloud per l'erogazione del servizio contrattualizzato. Nel caso vi siano anche dati personali (PII), METEDA assicura l'adempimento di quanto previsto dalla normativa vigente sul trattamento dei dati personali. Il cliente in qualsiasi momento può acquisire informazioni sull'elenco completo dei fornitori coinvolti facendo riferimento ai contatti identificati al punto sub 7.1) del presente documento.

9. SEPARAZIONE DEGLI AMBIENTI

La separazione dei diversi sistemi logici che coesistono su una infrastruttura Cloud è una delle principali misure per garantire la riservatezza e l'integrità dei dati memorizzati oltre che la sicurezza di tutta l'infrastruttura di erogazione del servizio.
Nel caso di servizi cloud acquisiti sul mercato, METEDA garantisce la separazione logica delle reti utilizzate da tutti i suoi clienti e, inoltre, anche la separazione tra la rete di gestione dell'infrastruttura e le reti destinate all'erogazione dei servizi.
Il fornitore esterno di cloud service dovrà fornire a METEDA, se richiesto, tutto il supporto necessario a verificare che tale segregazione sia garantita anche quando venissero richiesti elementi di segregazione addizionali nel rispetto delle proprie politiche.

10. GESTIONE DELLE IDENTITÀ DIGITALI

La gestione delle identità digitali deve rispettare quanto previsto nel documento "*P0L01_Politica di gestione degli accessi*"

11. GESTIONE DEI LOG

Quando METEDA utilizza servizi di Cloud Pubblico di terzi, deve rispettare quanto previsto nella procedura di riferimento per i sistemi in gestione e concordare con il fornitore le caratteristiche dei log necessari.
Nel caso METEDA operi in qualità di CSP, il servizio deve garantire ai suoi clienti: la possibilità di definire puntualmente i requisiti di monitoraggio in particolare per quanto riguarda tutte le operazioni che richiedono privilegi amministrativi; la tracciabilità delle operazioni attraverso la registrazione delle stesse in un file xml la cui retention è di 30 giorni.

12. BACKUP

METEDA nella gestione dei dati in cloud assicura l'esecuzione di backup plurimi ad intervalli temporali diversi. Il cliente in qualsiasi momento può acquisire informazioni di dettaglio sulle logiche di backup facendo riferimento ai contatti identificati al punto sub 7.1) del presente documento.

13. SICUREZZA DELLE APPLICAZIONI WEB

Nel caso di servizi cloud acquisiti sul mercato, METEDA ha a disposizione un team per gestire gli incidenti di sicurezza e adottare delle linee guida per lo sviluppo delle applicazioni Web che garantisca almeno le misure della procedura P 04CYB_ Requisiti Sviluppo Sicuro e della P 08.2 E_Gestione incidenti informatici e Data Breach.

14. DISASTER RECOVERY

Nel caso di servizi cloud acquisiti sul mercato, il fornitore qualificato per i servizi cloud deve adottare dei processi di gestione delle modifiche e di risposta agli incidenti conformi alle politiche di sicurezza definite da METEDA e coerenti con gli SLA contrattualizzati dei servizi erogati.

Il fornitore qualificato per i servizi cloud, inoltre, deve definire un piano di Disaster Recovery che garantisca il ripristino dei dati nelle tempistiche e con il livello di servizio contrattualizzato. Tale piano deve essere testato almeno una volta all'anno e il fornitore qualificato per i servizi cloud, su richiesta di METEDA, deve consegnare copia del rapporto di test.

15. INDAGINI INFORMATICHE

Ai clienti dei servizi cloud verrà garantito il massimo supporto, nel rispetto della normativa vigente, nel caso questi avviassero delle indagini sui servizi acquisiti.

Nel caso di servizi cloud acquisiti sul mercato, per consentire un'efficace attività di investigazione, deve essere concordata, con il fornitore qualificato per i servizi cloud, la modalità per la richiesta di dati necessari ad indagini interne ovvero a seguito di richiesta alle autorità legali competenti.

16. REQUISITI CONTRATTUALI

L'adozione dei servizi sul cloud a mercato possono comportare maggiori rischi rispetto all'integrità, riservatezza e disponibilità dei dati. Per questa ragione, i contratti che hanno come oggetto la fornitura di servizi su Cloud Pubblico, devono almeno prevedere:

- Una dichiarazione di "NDA - Non Disclosure Agreement";
- l'espressa dichiarazione che il cliente conserverà il diritto "esclusivo" alla proprietà dei dati per tutta la durata dell'accordo. La proprietà include tutte le copie dei dati disponibili presso il CSP, comprese eventuali copie dei supporti di backup;
- l'espresso divieto per il CSP di utilizzare i dati delle agenzie statali per marketing e/o pubblicità o qualsiasi altro scopo secondario non autorizzato;
- l'indicazione del paese(i) in cui è accettabile che i dati vengano conservati;
- che la normativa sulla protezione dei dati personali applicabile sia conforme alla normativa europea;
- il Service Level Agreement (SLA) del servizio;
- l'obbligo da parte del CSP di informare senza ingiustificato ritardo in merito a qualsiasi violazione dei dati, sia questa confermata o sospetta;
- l'obbligo per il CSP di eliminare completamente qualsiasi traccia di dati/informazioni, al termine dell'Accordo, da tutti i suoi sistemi;
- le modalità con cui il CSP restituirà i dati al termine dell'accordo.

I requisiti di cui sopra andranno rispettati anche nella contrattualizzazione di servizi quando METEDA opera in qualità di CSP verso i suoi clienti.

17. PRIVACY E TRATTAMENTO DEI DATI PERSONALI

A tutela dei diritti degli interessati i cui dati sono oggetto del trattamento, il cliente del servizio Cloud, in qualità di Titolare o Responsabile del trattamento, provvede a nominare il CSP, quale Responsabile o Sub-Responsabile del trattamento, con un atto formale.

METEDA si impegna a monitorare costantemente lo scenario in continua evoluzione di regolamenti e leggi riguardanti la privacy al fine di identificare i cambiamenti e determinare gli strumenti di cui i clienti potrebbero avere necessità per le esigenze di conformità, in funzione delle loro applicazioni.

METEDA si impegna ad informare costantemente i propri clienti su politiche, pratiche e tecnologie di sicurezza dei dati e di privacy applicate.
Questi impegni includono:

- Accesso e proprietà: il cliente conserva il pieno controllo dei propri contenuti. La proprietà dei dati rimane al cliente;

- Divulgazione dei contenuti dei clienti: METEDA non divulgherà i contenuti del cliente se non richiesto dalla legislazione vigente o da ordinanze vincolanti emesse da un'autorità statale;
- Controlli di Sicurezza: METEDA adotta politiche, standard e linee guida su privacy e protezione dei dati per raggiungere il più alto livello di sicurezza e confidenzialità.

18. MODALITA' DI AGGIORNAMENTO

Eventuali modifiche ai contenuti del presente documento sono comunicate ai clienti attraverso gli applicativi con accesso ad Internet o al servizio Cloud METEDA oppure, segnalate mediante il documento di rilascio alla prima release del software successiva alla modifica di cui in discorso.
La Versione aggiornata del presente documento è comunque sempre consultabile al sito internet www.meteda.it in calce alla Home Page.