

POLITICA DI SICUREZZA DELLE INFORMAZIONI NELL'EROGAZIONE DI SERVIZI CLOUD

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente documento definisce le politiche aziendali specifiche quali conseguenza della politica generale del Sistema di Sicurezza delle Informazioni definita dalla Direzione di WeTech's SPA SB relativamente al campo di applicazione definito relativo al servizio Cloud per la protezione dei dati globali, inclusi i dati personali applicando le best practices presenti nel settore normativo (ISO 27017, ISO 27018). La seguente politica, e le politiche aziendali derivanti da essa, viene rivista in caso di cambiamenti significativi o almeno una volta all'anno in occasione del riesame della Direzione eventualmente confermandone la validità.

2. DOCUMENTI DI RIFERIMENTO

- UNI EN ISO 27001:2022 - Sistemi di gestione per la sicurezza delle informazioni – Requisiti
- UNI EN ISO 27017:2018 - Codice di pratica per i controlli di sicurezza delle informazioni basati su ISO / IEC 27002 per i servizi cloud
- UNI EN 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 – D. Lgs. 196/2003 aggiornato dal D. Lgs. 101/2018 e s.m.i.)
- NIS2
- Codice etico

3. POLITICA DI SICUREZZA DI GESTIONE SERVIZIO CLOUD

3.1. POLITICA DI SICUREZZA DELLA GESTIONE DEL SERVIZIO CLOUD

Tutte le informazioni gestite da WeTech's SPA SB risiedono nella infrastruttura logica che compone il cloud. Tali informazioni possono essere riconducibili ai seguenti elementi:

- a) Elementi strutturali del cloud e loro configurazioni.
- b) Configurazione degli ambienti logici assegnati ai clienti.
- c) Informazioni e dati applicativi dei clienti stessi.

I dipendenti e collaboratori di WeTech's SPA SB hanno accesso esclusivamente alle informazioni al punto a) e b), mentre non hanno possibilità alcuna di accesso agli elementi di tipo c) se non dietro esplicita richiesta e permesso da parte del cliente per motivi di assistenza, manutenzione o aggiornamento. L'infrastruttura fisica nel suo complesso è protetta da firewall perimetrali che abilitano solo le porte strettamente necessarie ai servizi erogati.

L'accesso relativo a quanto descritto al precedente punto a) è possibile solo per gli Amministratori di Sistema incaricati WeTech's SPA SB con connessioni protette site-to-site o client-to-site SSL VPN.

L'accesso di amministrazione per i clienti relativo a quanto descritto nel punto b) è disponibile con connessioni protette e cifrate via HTTPS oppure in modalità client-to-site SSL VPN per i clienti che lo richiedono esplicitamente.

La sicurezza (riservatezza, integrità, disponibilità) dei dati viene garantita:

- dall'esterno l'azienda (es.: cyber attacchi)
- dall'interno all'azienda (es.: danni e azioni accidentali da parte del personale tecnico) dai seguenti punti 3.1.1 – 3.1.3, sotto il controllo del sistemista responsabile.

Tutte le informazioni applicative ed i relativi elaborati sono esclusiva responsabilità del cliente per quanto attiene il loro contenuto e il loro aggiornamento e rimangono sotto il controllo degli Amministratori di Sistema esclusivamente per quanto attiene l'integrità e la disponibilità.

Per consentire ai clienti di definire, eseguire e sfruttare l'ambiente di sicurezza fornito da WETECH'S, sono stati sviluppati programmi di controlli di sicurezza che implementa best practice di protezione della privacy e dati di livello globale. Queste procedure di sicurezza e controllo sono convalidate in modo indipendente tramite valutazioni di terze parti.

Il programma di controlli si basa sulla verifica, la dimostrazione e il monitoraggio:

- verifica che i servizi e le strutture di propria competenza prevedano un ambiente di controllo che funzioni in maniera efficace, attraverso policy, processi e attività di controllo, che comprende le persone, i processi e la tecnologia necessaria a definire e a gestire l'ambiente.
- dimostrazione della compliance di WeTech's SPA SB per contribuire a verificare la compliance del cliente rispetto ai requisiti governativi e di settore e per fornire informazioni sulle policy, sui processi e sui controlli definiti e gestiti;
- viene effettuato il monitoraggio per mantenere la compliance a standard globali e best practice, adottando requisiti nell'ambito dei controlli di sicurezza.

3.1.1. Programmi di controllo

WeTech's SPA SB identifica e definisce i programmi di controllo in base a certificazioni / attestazioni, leggi, regolamenti e privacy e allineamenti/quadri.

Le Certificazioni / attestazioni sono rilasciate da un organismo di audit di terza parte.

Le Leggi / regolamenti / privacy e allineamenti / quadri sono specifici in base al settore o alla funzione svolta.

Gli ambienti sono sottoposti a continue verifiche, mentre l'infrastruttura e i servizi sono approvati per l'utilizzo in base a diversi standard di compliance.

Tra questi:

ISO 27001: è uno standard di sicurezza globale ampiamente adottato che definisce i requisiti per i sistemi di gestione della sicurezza delle informazioni. Garantisce un approccio sistematico alla gestione delle informazioni dell'azienda e del cliente in base a valutazioni periodiche del rischio;

ISO 27017: fornisce orientamenti sugli aspetti di sicurezza informatica che riguardano il cloud computing e raccomandazioni riguardo all'implementazione di controlli sulla sicurezza delle informazioni specifici per il cloud, che integrano le linee guida delle norme ISO 27002 e ISO 27001. Questo codice di condotta fornisce indicazioni sull'implementazione dei controlli per la sicurezza delle informazioni che riguardano specificamente i fornitori di servizi cloud;

ISO 27018: è un codice internazionale delle best practice incentrato sulla protezione dei dati personali nel cloud. Si basa sullo standard ISO 27002 relativo alla sicurezza delle informazioni e fornisce indicazioni per l'implementazione dei controlli ISO 27002 che si applicano alle informazioni di carattere personale nel cloud pubblico;

La conformità di WeTech's SPA SB documenta che WeTech's SPA SB dispone di un sistema di controlli rivolto specificatamente a proteggere la privacy dei contenuti affidati dai clienti.

3.1.2. Sicurezza dei dati rispetto ai guasti hardware

L'infrastruttura logica abilitante, che consente la gestione delle informazioni descritte ai punti a), b) e c) è realizzata secondo modelli funzionali di alta affidabilità e ridondanza, che garantiscono copia e replica dei dati secondo politiche specifiche.

L'infrastruttura dei clienti è separata a livello logico da quella di produzione tramite VDOM, ed a livello fisico con Vcenter e Datastore dedicati, separati ed indipendenti.

3.1.3. Sicurezza del sistema rispetto all'intrusione

Le infrastrutture fisiche relative al cloud WeTech's SPA SB sono ospitate in ambienti fisici segregati ed indipendenti all'interno del data-Center. L'accesso al data center è gestito da un sistema di controllo accessi con badge.

Il gestore del data center è WeTech's SPA SB, in quanto situato nella sede legale dell'organizzazione (Via F.lli Alinari 76-80-82, Montevarchi (AR) dotato di certificazione ISO 27001.

3.1.4. Sicurezza al contorno

Al personale è fatto divieto:

- 1) Mantenere le sessioni di accesso alla infrastruttura aperte durante la loro assenza.
- 2) Conservare in qualunque forma scritta (es. salvato su file, su browser, scritto su foglio) le proprie credenziali di accesso alla infrastruttura fisica Wetechs, fatta eccezione per la password di superuser che è nota agli AdS di riferimento.

3.1.5. Sicurezza del Sistema rispetto a Malware

Il software installato in piattaforma è unicamente software di base (Linux, Apache, Tomcat, Windows, etc.) scaricato da sorgenti autenticate e con controllo di digest. Solo il sistemista responsabile ha le autorizzazioni per installare nuovo software.

3.2. 3.2 GESTIONE DEI DATI

I dati tecnologici dei clienti WeTech's SPA SB possono essere divisi in due categorie:

- Dati di Registrazione
- Dati di Archivio

WeTech's SPA SB ha adottato Il Modello di responsabilità condivisa, che è un paradigma di sicurezza che definisce ruoli e responsabilità e garantisce trasparenza tra i clienti e il provider di servizi cloud. La piattaforma di erogazione servizi cloud di WeTech's SPA SB è predisposta per l'erogazione di servizi di tipo IaaS, ognuno con diversi livelli di responsabilità. Per il dettaglio sulle funzionalità, modalità di erogazione del servizio, e sulle caratteristiche trasversali di qualità, sicurezza, privacy e continuità operativa del servizio, si rimanda alle condizioni specifiche del servizio.

I clienti dovrebbero valutare attentamente i servizi che scelgono in quanto le loro responsabilità varieranno in funzione dei servizi usati, dell'integrazione di quei servizi nel loro ambiente IT e delle leggi e normative applicabili.

IaaS

Per quanto riguarda il servizio IaaS, WeTech's SPA SB applica i controlli di seguito indicati:

- gestione e mantenimento dell'infrastruttura (fisico e infrastruttura cloud)
- attività di patching infrastrutturale (fisico e infrastruttura cloud)
- attività di configurazione infrastrutturale (fisico e infrastruttura cloud)
- formazione dei propri dipendenti.

Le restanti componenti (e la loro gestione) sono responsabilità del Cliente, inclusa la formazione dei dipendenti del Cliente.

3.2.1. Sicurezza dei contenuti

WeTech's SPA SB presta molta attenzione alla privacy dei suoi clienti. Il cliente resta sempre proprietario dei suoi contenuti mantenendo, tra l'altro, la possibilità di crittografarli, spostarli e gestirne la conservazione. WeTech's SPA SB fornisce strumenti che permettono di crittografare i dati in transito e inattivi, per garantire che solo gli utenti autorizzati possano accedervi, qualora gli venga richiesto dal cliente.

La struttura della nostra infrastruttura permette al cliente di mantenere il completo controllo sulla posizione geografica fisica in cui i dati sono ubicati, aiutandolo a soddisfare i requisiti in materia di posizione fisica dei dati.

WeTech's SPA SB non divulga i contenuti del cliente, salvo laddove sia richiesto dalla legislazione vigente o da ordinanze legali vincolanti emesse da un'autorità pubblica. Qualora WeTech's SPA SB fosse obbligata a divulgare i contenuti, verrà inviata una notifica preventiva al cliente per essere informato.

I data center di WeTech's SPA SB sono ubicati in Italia, per cui eseguire fisicamente lo storage dei dati è sempre sotto il controllo del cliente, il che semplifica la compliance ai requisiti territoriali e di posizione fisica dei dati.

3.2.2. Contenuti dei dati di Piattaforma

Possono essere raggruppati in 2 macro categorie.

3.2.3. Risorse assegnate al Cliente

Fanno parte di questa categoria le informazioni relative alle risorse definite nel contratto stipulato con WeTech's SPA SB ovvero:

- VPS
- Indirizzo IP del VPS
- Accesso protetto

3.2.4. Dati di accesso

Completata l'attivazione dell'ambiente del cliente (VPS) vengono fornite, al riferimento tecnico segnalato, le credenziali di accesso temporanee, con l'indicazione di cambiarle prima di procedere a qualsiasi attività.

Per questo motivo, nessun operatore WeTech's SPA SB, ha accesso all'ambiente e quindi ai dati sensibili interni alle VM (Virtual Machine) o agli applicativi del cliente, se non contrattualizzate in assistenza.

Controllo accesso logico: La sicurezza logica ha come obiettivo proteggere le informazioni ed i sistemi di elaborazione e di comunicazione con misure tecnologiche ed organizzative atte a garantire l'accesso ai sistemi in cloud a seguito di appropriata autorizzazione. La sicurezza logica viene attuata attraverso l'identificazione di un utente, l'autenticazione per permettere di verificare l'identità dell'utente e l'autorizzazione che abilita una serie di privilegi d'accesso, precedentemente individuati dal responsabile dell'utente (o, nel caso di utenze esterne, dal referente interno WeTech's).

I privilegi devono essere assegnati secondo principi di "need-to-know", ossia deve essere individuato il livello di permesso minimo sufficiente allo svolgimento dei compiti a cui l'utente è preposto.

La funzione IT provvederà operativamente alla registrazione dell'utente e ad impostare le autorizzazioni necessarie.

Quando un utente (dipendente o collaboratore) termina il rapporto di lavoro con WeTech's, le utenze ad esso associate devono essere tempestivamente disabilitate o eliminate (si rimanda alla 9_Wetechs SGI - PR08 Rev.4 procedura gestione risorse). Qualora le credenziali dell'utenza fossero condivise da più utenti verrà attivata la procedura di cambio password.

La funzione IT, aggiorna e manutiene le procedure di condivisione dati "Amministratori di Sistema WeTech's" con i clienti.

GESTIONE UTENZE GENERICHE: Per controllare il corretto accesso dell'utente vengono individuate le seguenti direttive che devono essere seguite dai referenti degli asset e dagli utenti.

Per i referenti (collaboratori WeTech's che gestiscono uno o più clienti): l'accesso ai dati ed agli strumenti utilizzati per il loro trattamento deve avvenire previa identificazione ed autenticazione da parte dell'utente tramite codice identificativo univoco (credenziali di accesso composte da user e password), che potrebbe essere condiviso da più collaboratori. Tale codice identificativo non può essere assegnato ad altri utenti, non autorizzati, neppure in tempi diversi.

L'autenticazione deve avvenire tramite una componente segreta; gli utenti devono essere in possesso di un opportuno profilo di autorizzazione che stabilisca quali operazioni possano essere effettuate sui dati (lettura, scrittura, cancellazione etc);

Periodicamente devono essere verificate le utenze per stabilire se sono ancora necessarie e opportunamente profilate. Le utenze inutilizzate da almeno sei mesi devono essere disabilitate.

Per gli utenti (clienti finali): gli utenti devono garantire la diligente custodia delle proprie credenziali d'accesso per assicurarne la segretezza e l'esclusivo utilizzo. Qualora si sospetti che la propria componente segreta sia stata divulgata, questa deve essere immediatamente cambiata; qualora gli utenti dovessero accedere in modo incidentale a sistemi cloud di WeTech's senza autorizzazione, sono tenuti a disconnettersi e segnalare l'anomalia alla funzione IT.

GESTIONE UTENZE AMMINISTRATIVE: Si definisce utenza amministrativa il profilo che ha accesso completo ad un sistema e/o a tutti i dati in esso contenuti.

Devono essere attuate le seguenti direttive:

- le utenze amministrative devono essere nominali, univocamente assegnate e appartenenti all'organico di;
- gli utenti con utenza amministrativa devono essere nominati Amministratori di Sistema in ottemperanza alle prescrizioni del Reg. UE 679/16 (Regolamento generale sulla protezione dei dati personali), del D.lgs. 196/03 (Codice in materia di dati personali) e dei provvedimenti dell'Autorità garante per la protezione dei dati personali 27 novembre 2008 - 25 giugno 2009;
- le utenze amministrative devono prevedere l'accesso ai soli sistemi di competenza e deve essere ridotto al minimo l'utilizzo di tali utenze;

Sono stabiliti i casi in cui viene assegnato l'accesso amministrativo ai singoli computer. La lista degli utenti con privilegi differenti da quelli standard deve essere periodicamente revisionata dal RSGI.

3.2.5. GESTIONE DEGLI ACCESSI

È necessario prevenire gli accessi non autorizzati ai server VPS, attraverso le seguenti direttive:

- Ai server si può accedere solo ed esclusivamente tramite la rete aziendale di WeTech's limitatamente alle postazioni autorizzate degli AdS specifici (con utenze amministrative), oppure presso il cliente;
- nel caso di una sessione scaduta o terminata in maniera anomala, cioè senza effettuare la chiusura mediante l'operazione di logoff/logout (ad esempio, in seguito ad una interruzione momentanea della linea di comunicazione), al riavvio della sessione di lavoro il sistema deve richiedere una nuova autenticazione dell'utente.

3.2.6. CREAZIONE E ASSEGNAZIONE CREDENZIALI DI ACCESSO AL CLIENTE

La gestione operativa del controllo degli accessi ai servizi cloud intesa come creazione, variazione, ripristino e cancellazione di un'utenza è di competenza della funzione AdS che sarà anche responsabile della consegna delle credenziali di accesso.

La funzione IT svolge i seguenti compiti:

- rilascia le credenziali per l'identificazione ed autenticazione per l'accesso alle applicazioni in maniera da impedire che uno stesso codice identificativo possa essere associato a due utenti differenti, neppure in tempi diversi;
- configura e gestisce i meccanismi di controllo degli accessi ai sistemi ed alle applicazioni in maniera che solo gli utenti autorizzati possano accedere;
- verifica periodicamente la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Gli utenti, all'atto della consegna delle credenziali di accesso, devono provvedere al cambio della password. Gli utenti hanno la responsabilità della gestione e conservazione delle password evitando di trascriverle su supporto cartaceo o elettronico e prevedendo un cambio in caso di sospetta compromissione. Le politiche sulle scadenze delle password sono gestite dal referente del cliente.

3.2.7. REVOCA DELLE CREDENZIALI DI ACCESSO

Nel caso di cambio delle mansioni lavorative o la cessazione del rapporto di lavoro, il responsabile dell'utente deve immediatamente informare la funzione IT che ha dato i privilegi per l'utente in questione. La funzione IT provvederà alla cancellazione/disabilitazione o modifica dell'utenza tracciando quanto avvenuto.

3.2.8. Dati di log

Il personale tecnico WeTech's SPA SB può accedere dati tecnici relativi all'utilizzo del servizio VPS Hosting dei vari clienti al solo scopo di monitorare il corretto funzionamento degli stessi e di conseguenza per analizzare e risolvere eventuali anomalie.

Trattandosi di log quali metriche VMware e utilizzo risorse, non riguardano dati sensibili dei clienti.

3.2.9. Gestione dei Dati Applicativi

WeTech's SPA SB non ha alcun accesso ai dati applicativi dei Clienti in quanto interni ad ogni singola VPS (Virtual Private Server).

WeTech's SPA SB ha solo visibilità sul numero e tipologia di VM (Virtual Machine) che ogni cliente ha, siano esse attive o spente, senza aver modo di accedere ai dati in esse contenuti sempre a meno sia in essere un contratto di assistenza.

3.2.10. Continuità operativa

L'infrastruttura prevede un elevato livello di disponibilità con il continuo controllo della capacità; i sistemi sono progettati per tollerare errori hardware o di sistema con un impatto minimo per il cliente.

Il disaster recovery è il processo di preparazione per affrontare e risolvere una situazione grave dove si intende qualsiasi evento che abbia un impatto negativo sulla continuità operativa; il cloud di WeTech's SPA SB supporta diverse architetture di Disaster recovery.

3.2.11. Backup per i servizi in cloud

La nostra azienda offre servizi cloud a una vasta gamma di clienti, ciascuno con esigenze specifiche di protezione dei dati. Per garantire la sicurezza e l'affidabilità dei servizi offerti, utilizziamo Veeam Backup & Replication per eseguire backup regolari delle VM ospitate su un'infrastruttura vCenter. Ogni cliente ha un proprio job di backup configurato per soddisfare le loro esigenze individuali, assicurando che i dati siano sempre protetti e facilmente recuperabili in caso di necessità.

Veeam Backup & Replication è una soluzione di protezione dei dati che offre backup e ripristino efficienti e affidabili per ambienti virtuali, fisici, NAS e cloud-native

Un team dedicato di tecnici verifica giornalmente lo stato dei backup, assicurando che ogni operazione sia completata correttamente e intervenendo prontamente in caso di problemi. Ad ogni modo tramite l'uso del vCenter il cliente può monitorare lo stato delle VM e dei job di backup.

3.3. CESSAZIONE DEL RAPPORTO DI LAVORO DEL PERSONALE WETECH'S SPA SB E/O DEI COLLABORATORI

Anche alla cessazione dell'attività, il dipendente o il collaboratore è tenuto alla riservatezza relativamente alle informazioni acquisite durante il rapporto di lavoro come definito dal contratto, dal codice (di comportamento) etico e Lettera applicazione SGSI ai Dipendenti e collaboratori.

3.4. CONTROLLI

I seguenti controlli sono effettuati periodicamente a campione:

1. Controllo del software installato nel sistema
2. Controllo dei log
3. Controllo a campione delle caratteristiche delle password (es. visionare la digitazione di un simbolo, o di una maiuscola o di un numero a richiesta del verificatore).
4. Verifica dei backup e della conservazione dello storico secondo policy.

Montevarchi, 24/02/2025

WETECH'S SPA SB
Via F.lli Alinari, 76/80/82
52025 MONTEVARCHI (AR)
Tel. 055.9850197 - Fax 055.9850208
P.IVA 05174160480 - CU. 6EWHWLT

Amministratore WETECH'S