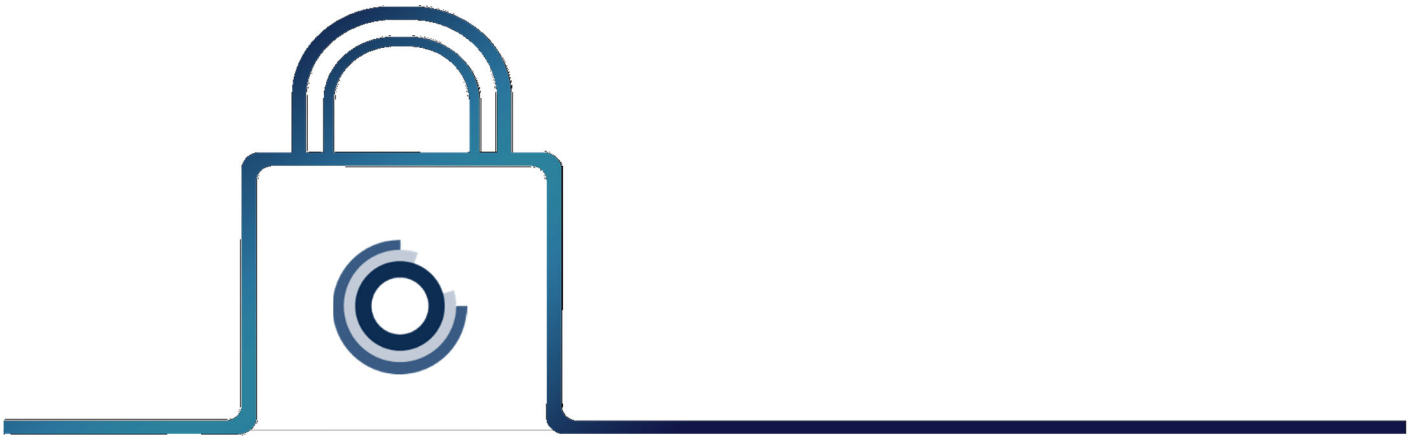
Direzione e Uffici:
Viale Pasteur, 45 – 00144 Roma
Tel. 06-5917534
www.opentech.it – info@opentech.it

Addendum – Misure di sicurezza per la tutela dei clienti di servizi SAAS erogati da Opentech



Sommario

INTRODUZIONE

L'insieme di dati ed informazioni trattate da Opentech S.r.l., a prescindere dalla forma con cui esse siano elaborate, gestite o archiviate, determina il Patrimonio Informativo aziendale che costituisce un elemento competitivo di fondamentale importanza sia per guidare le scelte tattiche/strategiche che per supportare i processi operativi aziendali.

Opentech attribuisce, quindi, al patrimonio informativo un valore strategico e rivolge pertanto una grande attenzione alla Sicurezza delle Informazioni proprie e/o conferite ad essa da dipendenti, clienti, fornitori ed altri attori esterni ed in generale di tutti i beni informativi che appartengono al perimetro aziendale, nel pieno rispetto del quadro normativo vigente, di legge e di settore.
Su tali basi, Opentech ha deciso di realizzare un Sistema di Gestione per la Sicurezza delle Informazioni (di seguito "SGSI") definito secondo regole e criteri previsti dalle "best practice" e dagli standard internazionali di riferimento, in conformità ai requisiti delle norme internazionali UNI EN ISO/IEC 27001, UNI EN ISO/IEC 27017 e UNI EN ISO/IEC 27018.
Lo scopo del presente documento è quello di descrivere, seppur in maniera sintetica, il parco di misure di sicurezza attuate da Opentech S.r.l. al fine di garantire ai propri clienti SAAS un servizio affidabile, conforme e sicuro.

1. Cloud SAAS

1.1 Misure di sicurezza organizzative

1.1.1 Policy e Disciplinari utenti: Opentech applica dettagliate policy e disciplinari, ai quali tutta l'utenza con accesso ai sistemi informativi ha l'obbligo di conformarsi e che sono finalizzate a garantire comportamenti idonei ad assicurare il rispetto dei principi di riservatezza, disponibilità ed integrità dei dati nell'utilizzo delle risorse informatiche.

1.1.2 Autorizzazione accessi logici: Opentech definisce i profili di accesso nel rispetto del least privilege necessari all'esecuzione delle mansioni assegnate. I profili di autorizzazione sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti.

1.1.3 Gestione interventi di assistenza: Gli interventi di assistenza son regolamentati allo scopo di garantire l'esecuzione delle sole attività previste contrattualmente e impedire il trattamento eccessivo di dati personali la cui titolarità è in capo al Cliente o all'Utente Finale

1.1.4 Valutazione d'impatto sulla protezione dei dati: Opentech ha predisposto una propria metodologia per l'analisi e la valutazione dei trattamenti allo scopo di procedere con la valutazione dell'impatto sulla protezione dei dati personali prima di iniziare il trattamento. In considerazione del Servizio erogato, e quindi delle Informazioni

trattate, viene identificato il livello della sicurezza, garantito dai controlli previsti, che deve essere applicato. Tale valutazione viene svolta periodicamente in fase di Risk assessment e, nel caso dell'adozione di nuovi sistemi informativi, prima della messa in opera.

1.1.5 Incident Management - Opentech ha realizzato una specifica procedura di Incident Management allo scopo di garantire il ripristino delle normali operazioni di servizio nel più breve tempo possibile, garantendo il mantenimento dei livelli migliori di servizio.

1.1.6 Data Breach - Opentech ha implementato un'apposita procedura finalizzata alla gestione degli eventi e degli incidenti con un potenziale impatto sui dati personali che definisce ruoli e responsabilità, il processo di rilevazione (presunto o accertato), l'applicazione delle azioni di contrasto, la risposta e il contenimento dell'incidente / violazione nonché le modalità attraverso le quali effettuare le comunicazioni delle violazioni di dati personali al Cliente.

1.1.7 Formazione: Opentech eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento corsi di formazione sulla corretta gestione dei dati personali.

1.1.8 Change Management: - Per quanto di propria competenza, Opentech ha in essere una specifica procedura attraverso la quale regolamenta il processo di Change Management in considerazione dell'introduzione di eventuali innovazioni tecnologiche o cambiamenti della propria impostazione e della propria struttura organizzativa. Opentech utilizza ambienti di Test per verificare l'impatto di modifiche ai sistemi o alle applicazioni che costituiscono i servizi cloud erogati da Opentech stessa. L'applicazione di aggiornamenti del sistema e delle applicazioni viene calendarizzata durante la giornata lavorativa per gli ambienti di Sviluppo e di Test, mentre è schedulata prevalentemente al di fuori dell'orario lavorativo per gli ambienti di Produzione. Sono previste soluzioni tecnologiche che permettano la disattivazione dei servizi e consentono il roll-back in caso di problemi durante la fase di aggiornamento o installazione. Opentech comunica ai clienti eventuali periodi di interruzione del servizio, con l'opportuno tempo di preavviso.

1.1.9 Politica per lo sviluppo sicuro: Opentech applica una politica per lo Sviluppo sicuro conforme alle linee guida AGID; tale politica contiene linee guida relative al ciclo di vita del software, alla scelta di Architetture e soluzioni tecnologiche, alla gestione del codice sorgente, alle metodologie di test. Sono presenti indicazioni relative allo sviluppo di Database di Frontend e di Backend, reportistica, alla realizzazione di API. Opentech verifica periodicamente l'applicazione di queste linee guida.

1.1.10 Gestione degli incidenti di sicurezza: Gli eventi e incidenti riferibili alla sicurezza delle informazioni sono individuati nel contesto delle attività operative quotidiane e sono documentati e gestiti come da specifica procedura. Gli incidenti con alta rilevanza (causata dalla tempistica del disservizio, dalla categoria di informazioni trattate, dalla presenza di dati personali) vengono comunicate ai clienti impattati dal servizio, entro 48 dal momento in cui Opentech ne è venuta a conoscenza. Anche i clienti dei servizi erogati da Opentech sono coinvolti nella individuazione e segnalazione degli eventi

e incidenti per la sicurezza delle informazioni tramite il servizio di helpdesk helpdesk@opentech.it, oppure l'indirizzo e-mail dedicato itsecurity@opentech.it.

1.1.11 Identificazione della legislazione applicabile: Opentech, tramite la formazione ed il costante aggiornamento delle proprie risorse, assicura che vengano rispettati i requisiti essenziali della normativa vigente all'epoca del progetto. In caso di necessità, Opentech può avvalersi della collaborazione di legali esterni che supportino l'azienda nell'individuazione e applicazione di specifiche norme.

1.2 Misure di sicurezza tecniche

1.2.1 Controlli crittografici: Le informazioni che transitano da e verso i server è protetta utilizzando i protocolli HTTPS e SFTP, con una verifica periodica del livello di sicurezza delle chiavi utilizzate per la codifica. Le informazioni sono memorizzate all'interno di Database protetti da sistemi crittografici (SQL Server TDE) e le chiavi di codifica delle postazioni possono essere conservate dal Responsabile delle IT Operations in uno spazio sicuro da lui gestito. Alternativamente è possibile utilizzare come soluzione alternativa uno spazio personale del dipendente posto in un'area sicura di Office 365. Per quanto riguarda le VPN le chiavi sono gestite direttamente dagli apparati. Le chiavi relative ai certificati HTTPS e SFTP sono comunicate ai soli tecnici e sistemisti autorizzati ad operare in tal senso.

1.2.2 Protection from malware: I sistemi sono protetti contro il rischio di intrusione dell'azione di programmi mediate l'attivazione di idonei strumenti elettronici aggiornati con cadenza periodica. Sono in uso strumenti antivirus mantenuti costantemente aggiornati.

1.2.3 Credenziali di autenticazione: I sistemi sono configurati con modalità idonee a consentirne l'accesso unicamente a soggetti dotati di credenziali di autenticazione che ne consentono la loro univoca identificazione.

1.2.4 Logging: I sistemi sono configurati con modalità che consentono il tracciamento degli accessi e delle attività svolte in capo alle diverse tipologie di utenti.

1.2.5 Backup & Restore: Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati. Opentech ha in essere una specifica procedura attraverso la quale regolamenta il processo di Back up e Restore. Con riferimento ai servizi erogati, Opentech tiene in considerazione la distinzione tra ambienti di Sviluppo, Test e Produzione ed attiva delle procedure di backup proporzionali alla criticità delle informazioni. Tali backup possono essere svolti in locale (sullo stesso server in cui si trovano dati o applicazioni), su cloud (in altra sede geografica) oppure tramite full backup del server. Periodicamente viene svolta una verifica della configurazione dei backup dei server. Le evidenze di queste attività sono gestite attraverso un apposito registro

1.2.6 Vulnerability Assessment & Penetration Test: Opentech effettua periodicamente attività di analisi delle vulnerabilità finalizzate a rilevare lo stato di esposizione alle vulnerabilità note, sia in relazione agli ambiti infrastrutturali sia a quelli applicativi,

considerando i sistemi in esercizio o in fase di sviluppo. Ove ritenuto appropriato in relazione ai potenziali rischi identificati, tali verifiche sono integrate periodicamente con apposite tecniche di Penetration Test, mediante simulazioni di intrusione che utilizzano diversi scenari di attacco, con l'obiettivo di verificare il livello di sicurezza di applicazioni/sistemi/reti attraverso attività che mirano a sfruttare le vulnerabilità rilevate per eludere i meccanismi di sicurezza fisica/logica ed avere accesso agli stessi. I risultati delle verifiche sono puntualmente e dettagliatamente esaminati per identificare e porre in essere i punti di miglioramento necessari a garantire l'elevato livello di sicurezza richiesto. Le evidenze di queste attività sono gestite attraverso un apposito registro.

1.2.7 Amministratori di Sistema: Relativamente a tutti gli utenti che operano in qualità di Amministratori di Sistema, il cui elenco è mantenuto aggiornato e le cui funzioni attribuite sono opportunamente definite in appositi atti di nomina, è gestito un sistema di log management finalizzato al puntuale tracciamento delle attività svolte ed alla conservazione di tali dati con modalità inalterabili idonee a consentirne ex post il monitoraggio. L'elenco degli Amministratori di Sistema è sottoposto ad attività di verifica in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto a trattamenti dei dati personali previsti dalle norme vigenti.

1.2.8 Registrazione e de-registrazione degli utenti: L'interfaccia di amministrazione delle soluzioni cloud fornite da Opentech, contengono funzionalità necessarie a consentire agli Amministratori del sistema individuati dal Cliente, di registrare, cancellare utenti ed attribuire profili di accesso e privilegi. Alcuni contesti di utilizzo prevedono delle integrazioni con il Sistema informativo del Cliente, tali da consentire una gestione integrata degli utenti e da automatizzare le operazioni di registrazione e cancellazione di utenti.

1.2.9 Gestione delle informazioni segrete di autenticazione degli utenti: Nei contesti in cui i servizi non prevedono un'autenticazione integrata, le informazioni segrete per l'autenticazione dell'utente sono memorizzate utilizzando algoritmi di codifica e di hash. In tal modo anche gli amministratori del sistema ed i tecnici della manutenzione hanno la possibilità di reimpostare la password ma non possono conoscere i dati relativi all'autenticazione. Nei contesti ove viene utilizzata un'autenticazione integrata, i servizi cloud erogati da Opentech non contengono alcuna informazione segreta di autenticazione, che rimane custodita nei sistemi del Cliente.

1.2.10 Segregazione delle reti: Gli ambienti cloud utilizzati per Sviluppo e Test sono collocati su una rete segregata rispetto agli ambienti per la Produzione, e sono protetti da VPN per le attività di amministrazione. La gestione degli utenti e dei privilegi è organizzata per gruppi, per identificare le risorse umane che hanno accesso alle aree di Produzione dei servizi erogati da Opentech. I servizi cloud erogati per i clienti fanno uso di installazioni separate ed indipendenti per ogni cliente, per garantire la completa segregazione dei tenant.

1.3 Data center

1.3.1 Misure di sicurezza: L'ambiente di virtualizzazione è presente su server ospitati in data center siti all'interno dell'Unione Europea, la cui gestione è demandata a fornitori certificati ISO 27001. Più precisamente, i data center di riferimento sono quelli di Microsoft Azure nella regione "West Europe". Per le misure di sicurezza fisica si prega di fare riferimento alle informazioni rese disponibili dal provider: https://docs.microsoft.com/it-it/azure/security/fundamentals/physical-security.

1.3.2 Accesso fisico: L'accesso al Data Center è limitato ai soli soggetti autorizzati e si fa rinvio alle misure di sicurezza indicate per i servizi di data center gestiti da Microsoft: https://www.microsoft.com/en-us/trust-center.

1.3.3 Dismissione sicura o riutilizzo delle apparecchiature: Si fa rinvio alle linee guida di Microsoft per la gestione delle apparecchiature all'interno dei data center Microsoft: https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-bearing-device-destruction