



Sistema Gestione Qualità e Sicurezza delle Informazioni Certificati
UNI EN ISO 9001 N°9151H&SQ
UNI EN ISO 13485 N°9124H&SM
ISO 27001 N°9194H&SS
IT - 65007

CARTA DEI SERVIZI CLOUD H&S SPA

(revisione 01 del 04/05/2020)

1. PREMESSA

La presente carta dei servizi è stata redatta in relazione alla certificazione ISO 27001 e alle linee guida delle norme ISO 27017 e 27018

H&S SPA aggiorna periodicamente la Carta alla luce delle modifiche relative alle modalità di offerta dei servizi al Cliente ed alle variazioni legislative e tecniche del settore. La Carta aggiornata è adeguatamente divulgata in formato elettronico sul sito web www.hes.it e in formato cartaceo ove richiesto.

La Carta dei Servizi definisce gli impegni della società nei confronti dei Clienti e i loro diritti in relazione alla fornitura dei servizi Cloud contrattualmente previsti. Attraverso questo documento H&S SPA si impegna:

- ad operare per ottenere un continuo miglioramento dei propri standard di qualità;
- a semplificare, potenziare e rendere più trasparente il proprio rapporto col Cliente.

La presente Carta dei Servizi, ferme restando le specifiche disposizioni previste nei contratti, è vincolante per H&S SPA nei confronti dei Clienti e costituisce il punto di riferimento nei rapporti con gli stessi.

2. PRINCIPI FONDAMENTALI

L'obiettivo del Sistema di Governo per la Sicurezza delle Informazioni di H&S SPA è di garantire un adeguato livello di sicurezza dei dati e delle informazioni nell'ambito della progettazione, sviluppo ed erogazione dei servizi aziendali (compresi i servizi cloud), attraverso l'identificazione, la valutazione ed il trattamento dei rischi ai quali i servizi stessi sono soggetti.

Tutte le informazioni, che vengono create o utilizzate dall'Azienda sono da salvaguardare e debbono essere protette, secondo la classificazione attribuita, dalla loro creazione, durante il loro utilizzo, fino alla loro eliminazione. Le informazioni sono gestite in modo sicuro, accurato e affidabile e debbono essere prontamente disponibili per gli usi consentiti.

Il Sistema di Governo per la Sicurezza per le Informazioni di H&S SPA definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sotto elencati requisiti di sicurezza di base:

- **Riservatezza**, ovvero la proprietà dell'informazione di essere nota solo a chi ne ha i privilegi;
- **Integrità**, ovvero la proprietà dell'informazione di essere modificata solo ed esclusivamente da chi ne possiede i privilegi;
- **Disponibilità**, ovvero la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che ne godono i privilegi.

H&S SPA inoltre si impegna a raggiungere la conformità con la legislazione applicabile sulla protezione delle "Personally Identifiable Information (PII)" e a rispettare le condizioni contrattuali concordate con il cliente in tale ambito

Per un maggior dettaglio si veda la Politica Aziendale della Sicurezza delle Informazioni

3. PARAMETRI DI QUALITÀ

Nello svolgimento della propria attività H&S SPA rivolge la massima attenzione al grado di soddisfazione della clientela ponendosi obiettivi sempre più ambiziosi in termini di qualità dei servizi offerti.

In un'ottica di miglioramento continuo e di centralità del cliente l'azienda adotta una serie di indicatori stabilendo annualmente degli obiettivi da raggiungere in base ai quali valutare periodicamente il livello qualitativo conseguito.

4. OBBLIGHI E LIMITAZIONI DI RESPONSABILITÀ DI H&S SPA - OBBLIGHI E DIRITTI DEL CLIENTE

H&S SPA offre i servizi Cloud studiando sempre le soluzioni più idonee ad ogni realtà.

I servizi che compongono l'offerta di H&S SPA sono resi nella massima trasparenza nei confronti della clientela attraverso i contratti a cui si rimanda per tutte le clausole contrattuali.

Si sottolinea comunque quanto segue:

- H&S SPA si impegna a fornire un servizio cloud che non comporti la riduzione delle misure di sicurezza senza l'approvazione del cliente
- Il cliente accetta tutte le procedure messe in atto da H&S SPA per la gestione del servizio
- Risoluzione controversie tra clienti: si vedano le condizioni contrattuali
- Divulgazioni di informazioni personali a terzi: si vedano gli accordi di riservatezza.
- Fornitori/sub appaltatori che possono o ricevono dati del cliente:
 - Fornitori di backup esterno (es: Istituto di Vigilanza, Notaio, Google)
 - Vodafone, Telecom, AgileTelecom, WhatsApp per servizi di messaggistica aziendale
 - Fornitori di Disaster Recovery

5. ASPETTI GENERALI DEL SERVIZIO

Di seguito vengono definiti in linea generale i seguenti aspetti di gestione del servizio cloud (per ulteriori dettagli si faccia riferimento al contratto oppure il cliente può far richiesta della documentazione di dettaglio ad H&S SPA):

- malware protection: i servizi e gli apparati utilizzati per lavorare su server/device o altro che acceda ai servizi stessi sono protetti da AntiVirus e AntiMalware integrati e centralizzati.
- backup: H&S utilizza un doppio sistema di backup per i dati presenti, con archivio mensile della produzione e retention. È inoltre attiva l'esportazione settimanale del backup presso un ente di sorveglianza che custodisce lo stesso in sale adeguate.
- cryptographic controls: l'accesso ai servizi è garantito tramite crittografia TLS.
- vulnerability management: vengono generati report di vulnerabilità atti a mantenere i servizi sempre disponibili con le configurazioni più aggiornate possibile.
- incident management: la gestione degli incidenti vengono gestiti secondo procedura documentata, tracciati in un sistema di ticketing / gestione delle non conformità e azioni correttive secondo tempistiche, modalità e responsabilità definite, comprese quelle verso il cliente.
- technical compliance checking, security testing: vengono applicati tutti i requisiti delle ISO/IEC 27001, 27017 e 27018 e verificati periodicamente
- auditing: H&S SPA è certificata ISO 27001 ed è sottoposta ad audit annuale da parte dell'ente di certificazione e svolge periodicamente audit interni secondo una procedura documentata.
- collection, maintenance and protection of evidence, including logs and audit trails; protection of information upon termination of the service agreement: un software aziendale raccoglie le informazioni necessarie per le operazioni di verifica schedate. I dati sottostanno al regolamento UE 2016/679 (GDPR)
- authentication and access control; identity and access management: la configurazione dei servizi Active Directory integrati di Windows garantiscono i livelli di sicurezza necessari. Ove non presente l'integrazione con Windows AD i sistemi vengono configurati ad-hoc. Le configurazioni sono documentate in PO.HS.4.2-2.
- informazioni al cliente del servizio cloud in merito alla protezione dei record raccolti e archiviati dal H&S SPA in relazione all'uso dei servizi cloud da parte del cliente del servizio cloud: I dati sottostanno al regolamento UE 2016/679 (GDPR)
- informazioni sulle modalità per la restituzione e la rimozione delle risorse di qualsiasi cliente del servizio cloud al termine dell'accordo per l'uso di un servizio cloud: I dati sottostanno al regolamento UE 2016/679 (GDPR)

6. TUTELA DELLA PRIVACY

Ai sensi del Regolamento UE 2016/679 in materia di Protezione delle persone fisiche con riguardo al trattamento dei dati personali, H&S SPA garantisce la massima riservatezza delle informazioni fornite dai clienti, le quali non potranno essere utilizzate, salvo il consenso diretto dell'interessato o la richiesta delle autorità competenti, per le finalità diverse dall'erogazione e fatturazione del servizio.

L'informativa completa è disponibile al seguente link: <https://www.hes.it>.