CAPITOLATO di SICUREZZA delle INFORMAZIONI Per FORNITORI ICT di GILARDONI S.p.A. a Socio Unico

SOMMARIO

1. SCOPO 2
2. CAMPO DI APPLICAZIONE 2
3. PRINCIPI GENERALI DI SICUREZZA 2
4. GESTIONE DELLE INFORMAZIONI 2
5. GESTIONE DEGLI ACCESSI AI SISTEMI 2
6. GESTIONE DEGLI INCIDENTI DI SICUREZZA 2
7. GESTIONE DELLE MODIFICHE 3
7.A. SVILUPPO E MANUTENZIONE DI SISTEMI (SE APPLICABILE) 3
7.B. SVILUPPO SOFTWARE DI PRODOTTO (SE APPLICABILE) 3
8. GESTIONE DEI SUBFORNITORI 3
9. CONTINUITÀ OPERATIVA 4
10. VERIFICHE E AUDIT 4
11. PROTEZIONE DEI DATI PERSONALI 4
12. RESTITUZIONE O CANCELLAZIONE DELLE INFORMAZIONI 4
13. ACCETTAZIONE DEL CAPITOLATO 4

1. SCOPO

Il presente capitolato definisce i requisiti minimi di sicurezza delle informazioni che devono essere rispettati dai fornitori che, nell'ambito delle attività svolte per GILARDONI:

- trattano informazioni aziendali,
- accedono ai sistemi informativi
- o forniscono prodotti o servizi ICT.

L'obiettivo del presente documento è garantire che le attività svolte dal fornitore non compromettano la **riservatezza, l'integrità e la disponibilità delle informazioni e dei sistemi di GILARDONI**.

2. CAMPO DI APPLICAZIONE

Il presente capitolato si applica ai fornitori che:

- forniscono prodotti o servizi ICT;
- accedono ai sistemi informativi o alle infrastrutture di rete di GILARDONI;
- trattano o possono accedere a informazioni aziendali o dati trattati da GILARDONI;
- supportano servizi o processi aziendali che possono influire sulla sicurezza delle informazioni o sulla continuità operativa ICT.

Il presente capitolato costituisce parte integrante della documentazione contrattuale applicabile al rapporto di fornitura.

3. PRINCIPI GENERALI DI SICUREZZA

Il fornitore si impegna a:

- proteggere le informazioni ricevute o trattate per conto di GILARDONI;
- adottare misure adeguate a prevenire accessi non autorizzati, perdita o divulgazione delle informazioni;
- utilizzare le informazioni esclusivamente per le finalità previste dal rapporto contrattuale;
- garantire che il personale coinvolto nelle attività sia adeguatamente formato e vincolato da obblighi di riservatezza.

Le informazioni fornite da GILARDONI non possono essere condivise con terze parti senza preventiva autorizzazione.

4. GESTIONE DELLE INFORMAZIONI

Il fornitore deve adottare misure adeguate a garantire la protezione delle informazioni trattate nell'ambito delle attività svolte per GILARDONI.

In particolare, deve:

- proteggere le informazioni da accessi non autorizzati;
- evitare perdita, divulgazione o alterazione delle informazioni;
- garantire la protezione delle informazioni anche durante la trasmissione o l'archiviazione.

Le informazioni di GILARDONI devono essere gestite secondo principi di **riservatezza e limitazione dell'accesso**.

5. GESTIONE DEGLI ACCESSI AI SISTEMI

Qualora il fornitore debba accedere ai sistemi informativi o alle infrastrutture di GILARDONI, devono essere rispettati i seguenti principi:

- gli accessi sono concessi esclusivamente al personale autorizzato;
- gli accessi devono essere limitati alle attività strettamente necessarie;
- le credenziali di accesso devono essere personali e non condivise;
- gli accessi devono essere revocati quando non più necessari.

Il fornitore deve adottare misure adeguate a proteggere le credenziali di accesso e prevenire utilizzi non autorizzati.

6. GESTIONE DEGLI INCIDENTI DI SICUREZZA

Il fornitore deve comunicare tempestivamente a GILARDONI eventuali incidenti di sicurezza che possano coinvolgere:

- informazioni aziendali trattate per conto di GILARDONI;
- sistemi informativi o infrastrutture utilizzate per l'erogazione del servizio;
- dati o servizi forniti a GILARDONI.

La comunicazione deve avvenire senza ritardo e includere, ove disponibile:

- descrizione dell'incidente;
- informazioni coinvolte;
- misure adottate per contenere o gestire l'evento.

7. GESTIONE DELLE MODIFICHE

Il fornitore deve comunicare preventivamente a GILARDONI eventuali modifiche che possano influire sui servizi forniti o sulla sicurezza delle informazioni.

In particolare, devono essere comunicati cambiamenti relativi a:

- infrastrutture o sistemi utilizzati per il servizio;
- tecnologie o piattaforme utilizzate;
- organizzazione o personale chiave coinvolto nel servizio;
- subfornitori coinvolti nell'erogazione del servizio.

Le modifiche devono essere verificate prima della loro implementazione in ambiente di produzione.

7.a. SVILUPPO E MANUTENZIONE DI SISTEMI (SE APPLICABILE)

Nel caso in cui il fornitore svolga attività di sviluppo, configurazione o manutenzione di software, sistemi o soluzioni ICT per conto di GILARDONI, devono essere garantiti i seguenti requisiti:

- le attività devono essere eseguite sulla base di requisiti definiti e condivisi con GILARDONI;
- le modifiche devono essere tracciate e, ove applicabile, preventivamente autorizzate;
- devono essere effettuate verifiche sulle modifiche prima del rilascio;
- deve essere garantita la gestione delle versioni e dei rilasci;
- GILARDONI si riserva la possibilità di richiedere evidenze e svolgere verifiche;
- devono essere adottate misure di sicurezza durante lo sviluppo (es. gestione accessi, separazione ambienti, protezione dati).

7.b. SVILUPPO SOFTWARE DI PRODOTTO (SE APPLICABILE)

Per i fornitori di sviluppo software, devono essere rispettate inoltre le seguenti indicazioni:

- utilizzare i relativi software esclusivamente per l'esecuzione delle mansioni contrattualizzate;
- fivieto di accesso al codice sorgente di programmi proprietari di GILARDONI non necessari, di effettuare operazioni di reverse-engineering, modificare, decriptare, decompilare, estrarre il software utilizzato e convertire il linguaggio del software in formato leggibile;
- non copiare, tradurre, modificare, adattare o creare opere derivate da codici sorgente o dai contenuti dei repository di GILARDONI;
- non interferire con il corretto funzionamento di misure di crittografia e, in particolare, a non tentare di aggirare la sicurezza, eludere i sistemi di gestione delle licenze o altri meccanismi di protezione dei codici sorgente e dei repositories dei codici;
- non concedere a soggetti non autorizzati alcun diritto relativamente programmi software sviluppati da GILARDONI;
- non oscurare, modificare o rimuovere avvisi di copyright, marchi, segni o altri diritti della proprietà intellettuale o a porvi avvisi sopra o visibili durante l'utilizzo di programmi software proprietari di GILARDONI.

8. GESTIONE DEI SUBFORNITORI

Qualora il fornitore utilizzi subfornitori per l'erogazione del servizio o per lo sviluppo, la gestione o la manutenzione delle soluzioni fornite a GILARDONI, deve garantire che tali soggetti rispettino requisiti adeguati di sicurezza delle informazioni.

In particolare, il fornitore deve:

- valutare i subfornitori coinvolti nelle attività rilevanti per il servizio fornito;
- definire nei confronti dei subfornitori requisiti di sicurezza delle informazioni coerenti con quelli applicabili al presente capitolato;
- monitorare, ove applicabile, il rispetto di tali requisiti.

Il fornitore deve inoltre comunicare preventivamente a GILARDONI l'eventuale coinvolgimento di nuovi subfornitori nelle attività relative ai servizi o ai prodotti forniti.

In particolare, devono essere comunicati cambiamenti relativi a:

- introduzione di nuovi subfornitori coinvolti nel servizio;
- sostituzione di subfornitori precedentemente utilizzati;
- trasferimento delle attività verso nuovi soggetti o infrastrutture gestite da terzi.

Tali modifiche devono essere valutate da GILARDONI prima della loro implementazione, al fine di verificare eventuali impatti sulla sicurezza delle informazioni o sulla continuità del servizio.

Qualora il subfornitore tratti dati personali per conto di GILARDONI, il fornitore deve garantire che siano applicate condizioni di protezione dei dati equivalenti a quelle previste per il fornitore principale e che siano rispettati gli obblighi previsti dalla normativa applicabile in materia di protezione dei dati personali.

Il fornitore rimane in ogni caso **responsabile nei confronti di GILARDONI** delle attività svolte dai propri subfornitori.

9. CONTINUITÀ OPERATIVA

Il fornitore deve adottare misure adeguate a garantire la continuità del servizio fornito a GILARDONI.

Devono essere previste, ove applicabile:

- misure di prevenzione delle interruzioni del servizio;
- procedure di gestione di eventuali incidenti o indisponibilità;
- tempi di ripristino coerenti con gli accordi contrattuali.

10.VERIFICHE E AUDIT

GILARDONI può richiedere al fornitore evidenze documentali o informazioni relative alle misure di sicurezza adottate.

Quando necessario, possono essere effettuate verifiche o audit concordati con il fornitore al fine di verificare il rispetto dei requisiti previsti dal presente capitolato.

11.PROTEZIONE DEI DATI PERSONALI

Qualora il fornitore tratti **dati personali per conto di GILARDONI**, deve essere formalmente designato **Responsabile del trattamento** secondo quanto previsto dalla normativa sulla protezione dei dati personali.

In tali casi dovrà essere sottoscritto il **modulo aziendale *2B-1* – Nomina a Responsabile Esterno del Trattamento**.

Il fornitore si impegna a trattare i dati personali esclusivamente per le finalità previste e ad adottare adeguate misure di sicurezza per la loro protezione.

12.RESTITUZIONE O CANCELLAZIONE DELLE INFORMAZIONI

Alla cessazione del rapporto contrattuale o al termine delle attività svolte per conto di GILARDONI, il fornitore deve:

- restituire a GILARDONI tutte le informazioni, i dati e la documentazione ricevuti o generati nell'ambito delle attività svolte;
- cancellare o distruggere eventuali copie delle informazioni o dei dati conservati nei propri sistemi, salvo diversa richiesta o obbligo normativo.

Qualora richiesto da GILARDONI, il fornitore deve fornire evidenza dell'avvenuta restituzione o cancellazione delle informazioni.

Tale obbligo si applica anche alle eventuali copie delle informazioni detenute da **subfornitori coinvolti nelle attività**.

Nel caso in cui le attività svolte comportino il trattamento di **dati personali**, la restituzione o cancellazione dei dati deve avvenire nel rispetto della normativa applicabile in materia di protezione dei dati personali.

13.ACCETTAZIONE DEL CAPITOLATO

Il presente capitolato costituisce parte integrante della documentazione contrattuale tra **GILARDONI S.p.A.** e il Fornitore.

Con la sottoscrizione del presente documento, il fornitore dichiara di:

- ➡ aver preso visione dei requisiti di sicurezza delle informazioni definiti nel presente capitolato;
- ➡ impegnarsi al rispetto delle misure e delle condizioni applicabili nell'ambito delle attività svolte per GILARDONI;
- ➡ garantire che il personale coinvolto nelle attività sia informato dei requisiti applicabili e operi nel rispetto degli stessi.

Ragione Sociale: _____

Rappresentante autorizzato: _____

Ruolo: _____

Timbro e Firma Fornitore per accettazione

Luogo _____

Data _____ _____