Allegato 4 – Sicurezza informatica.

Conformità con le policy della Fondazione e la legislazione vigente
Il fornitore deve essere conforme e deve garantire che i suoi eventuali subfornitori rispettino i termini del contratto e la normativa vigente, in ogni momento durante la fornitura. Il fornitore deve garantire che i servizi siano erogati in modo tale che la Fondazione sia conforme alla legislazione vigente, in quanto la stessa conformità della Fondazione è dipendente dalla corretta e rigorosa erogazione dei servizi. Il fornitore deve tempestivamente fornire alla Fondazione ogni informazione o evidenza richiesta dallo stesso che sia in suo possesso o sotto il suo controllo al fine di garantire la conformità della Fondazione alla legislazione vigente. L'applicazione della presente clausola deve avvenire senza alcun costo aggiuntivo e/o onere alcuno a carico della Fondazione.

Clausola di manleva
Il Fornitore solleva la Fondazione da ogni responsabilità e risponde degli eventuali inadempimenti o violazioni di legge perpetrate da suoi collaboratori/ausiliari o terzi in relazione alla perdita, furto o diffusione non autorizzata di dati.

Misure minime di sicurezza
E' responsabilità del fornitore:

- implementare tutte le misure di sicurezza in conformità al Codice Privacy ed all'Allegato B al Codice Privacy (Disciplinare Tecnico in materia di misure minime di sicurezza), artt. da 33 a 36 del DLgs n. 196 del 30/06/2003, "Codice in materia di protezione dei dati";

- predisporre un piano delle sicurezza comprendete la periodicità dei vulnerabilty assesment, i piani di remediation, l'aggiornamento costante dei software, l'aggiornamento degli antivirus, l'installazione di security patch, l'adozione di sistemi di ATP (Advanced Threat Protection);

- garantire la crittografia dei dati;

- garantire il controllo degli accessi al proprio data center ;

- nominare, all'interno del suo organigramma, gli amministratori di sistema coinvolti nella gestione dei sistemi e ad implementare tutte le misure di sicurezza in conformità al Provvedimento del Garante della Privacy sull'operato degli amministratori di sistema con particolare riferimento all'archiviazione del log da esibire alla Fondazione su richiesta;

- riferire costantemente alla Fondazione lo stato di applicazione ed evoluzione delle misure di sicurezza adottate;

- informare tempestivamente la Fondazione di qualsiasi circostanza rilevante in relazione al trattamento dati.

- riferire costantemente alla Fondazione lo stato di applicazione ed evoluzione delle misure di sicurezza adottate;

Smaltimento sicuro dei dati
Il fornitore deve essere conforme e deve garantire che i suoi subfornitori rispettino la normativa vigente relativa allo smaltimento sicuro dei dati. Il fornitore deve definire delle istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati della Fondazione al fine di evitare accessi non autorizzati e trattamenti non consentiti. I supporti rimovibili se non utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
Il fornitore deve pertanto dotarsi di procedure e strumenti adeguati ad implementare lo smaltimento sicuro di ogni potenziale dato residuo presente sull'apparecchiatura/dispositivo da dismettere o da riassegnare ad altro utilizzatore, e deve produrre una certificazione di cancellazione relativa ad ogni supporto cancellato.

Audit

Il fornitore, una volta l'anno, deve garantire alla Fondazione il diritto di accesso alle sue strutture, ivi compreso qualsiasi sito da cui il fornitore esegua la sua attività e/o presso il quale compia operazioni di elaborazioni informatiche connesse all'esecuzione del presente contratto, compresi i siti dei suoi subfornitori, e ai sistemi informatici suoi e dei suoi fornitori, ivi compresi i sistemi di ripristino dati. Il fornitore deve garantire la fornitura di tutta l'assistenza necessaria e collaborazione da parte sua e dei suoi subfornitori nei confronti dell'auditor, compreso l'accesso controllato ai sistemi, documenti e qualsiasi altra informazione pertinente.

Gestione del rischio
Il fornitore deve adottare e seguire appropriate procedure di analisi del rischio sui servizi/soluzioni IT erogati. L'analisi del rischio dovrà essere condotta almeno annualmente ed i risultati dovranno essere condivisi con la Fondazione.

Disponibilità dei sistemi
Deve indicare con periodicità da concordare con la Fondazione i seguenti parametri relativi all'affidabilità e disponibilità dei sistemi:

- **Recovery Time Objective (RTO): tempo di ripristino in caso di distruzione del sistema**

- **Recovery Point Objective (RPO): perdita di dati in caso di ripristino del sistema valutata in termini di transazioni non rispristinabili.**

Gestione degli incidenti
Il Fornitore si impegna a definire con la Fondazione una procedura di escalation per gestire la risoluzione degli incidenti. La procedura prevede una modalità di comunicazione per informare il prima possibile la Fondazione su eventuali problemi che possono compromettere il servizio, azioni per gestirli, i rischi e le criticità conseguenti. Il fornitore deve:

- dare supporto alla fondazione anche in caso di incidenti rilevati dalla Fondazione;
- segnalare alla Fondazione incidenti rilevati aventi un impatto, anche potenziale, su sistemi e servizi a supporto dei processi della Fondazione, e relativa gestione, con particolare riferimento agli incidenti critici;
- produrre reportistica a supporto del processo di gestione incidenti;
- supportare la Fondazione nell'invio al Garante della Privacy delle comunicazioni relative ad eventuali violazioni dei dati (data breach) o incidenti informatici (accessi abusivi, azione di malware…) verificatesi sui dati della Fondazione.

Dispositivi collegati alle reti della Fondazione
Il collegamento di un dispositivo del Fornitore o subfornitore alla rete della Fondazione deve essere autorizzato dalla fondazione. Il fornitore è responsabile della messa in sicurezza del dispositivo con antivirus e patch per proteggere asset e informazioni della Fondazione. Qualsiasi dispositivo di proprietà del Fornitore che memorizza le informazioni della Fondazione, dove essere protetto anche crittografando le informazioni.

Accesso alle risorse della Fondazione
Solo gli utenti autorizzati dalla Fondazione per iscritto possono accedere alle informazioni e ai dati contenuti all'interno delle infrastrutture della fondazione (di proprietà o concesse in uso) o infrastrutture di terze parti utilizzate dalla Fondazione e situate in siti di soggetti terzi. Tutti gli accessi saranno concessi solo ai singoli individui. Account generici o condivisi sono assolutamente proibiti. Nessun dato o informazione contenuto all'interno dell'infrastruttura della Fondazione (di proprietà o concesse in uso) o in infrastrutture di terze parti utilizzate dalla fondazione e situate in siti di soggetti terzi devono essere comunicati a terzi senza previa autorizzazione scritta da parte della Fondazione. Il fornitore deve comunicare tempestivamente alla Fondazione quando un suo dipendente autorizzato all'accesso lascia l'azienda temporaneamente o definitivamente, o non necessità più dell'accesso, o sono cambiati ruolo/privilegi nell'accedere ai beni della Fondazione.

Quando il contratto è risolto per qualsiasi ragione o è scaduto, tutti gli accessi devono essere immediatamente revocati. Il fornitore non sarà ulteriormente autorizzato ad accedere alle risorse della Fondazione.

Accesso fisico ai locali della Fondazione
La Fondazione comunicherà le regole di sicurezza e di accesso ai propri siti. Il fornitore deve consegnare alla Fondazione una lista con i nomi e i ruoli del suo personale o del personale dei subfornitori che possono avere accesso a siti della Fondazione. Il personale del fornitore oppure il personale dei subfornitori inclusi in tale elenco devono presentarsi alla reception della Fondazione, dove verrà consegnato un badge, che dovrà essere indossato in modo visibile e in ogni momento durante la visita presso i siti della Fondazione. Se una persona non è inclusa nella lista per qualsiasi ragione e ha bisogno di accedere al sito della Fondazione, verrà registrata presso la reception dopo aver mostrato un suo documento d'identità. Tale persona deve essere accompagnata in ogni momento dal personale della Fondazione. Se il personale del fornitore o il personale dei subfornitori, ha bisogno di accedere alle aree riservate (come le sale server, data center, gli armadi di rete, etc.), esso deve essere accompagnato in ogni momento dal personale della Fondazione.

Obbligo di riservatezza
Sia per tutta la durata del contratto che successivamente il fornitore si obbliga a:

- non utilizzare le Informazioni per scopi diversi, in tutto o in parte, da quelli contemplati dal contratto;

- mantenere riservati i fatti, documenti, progetti, dati e informazioni (intesi nella più ampia accezione dei termini) di cui verrà a conoscenza e/o disporrà in relazione al e/o in esecuzione del presente contratto (di seguito: Informazioni);

Eccezioni
Qualsiasi deroga alle disposizioni definite in queste clausole deve essere valutata ed eventualmente concessa dalla Fondazione in forma scritta.

- non divulgare o altrimenti rendere note a terzi le Informazioni, in mancanza di specifica autorizzazione o accordo.