ALLEGATO A
MODELLO PER LA PRE-VALUTAZIONE DEL RISCHIO

A. VALUTAZIONE DEI RISCHI E DELL'IMPATTO DEL TRATTAMENTO

N.	DOMANDE SU IMPATTO	VALORI				MOTIVAZIONE
1	In caso di mancata riservatezza dei dati personali – divulgazione non autorizzata – quale è l'impatto sugli interessati?	**BASSO**	**MEDIO**	**ALTO**	**MOLTO ALTO**	
2	In caso di mancata integrità dei dati personali – alterazione non autorizzata – quale è l'impatto sugli interessati?					
3	In caso di mancata disponibilità dei dati personali – perdita o distruzione non autorizzata – quale è l'impatto sugli interessati?					

LEGENDA: COME INTERPRETARE I VALORI DI IMPATTO?

- **BASSO** = l'impatto è basso quando gli interessati andranno incontro a disagi minori che supereranno senza problemi (tempo trascorso reinserendo le informazioni, fastidi, irritazioni, etc.);
- **MEDIO** = l'impatto è medio quando gli interessati possono avere significativi disagi che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di acceso ai servizi aziendali, paura, stress, mancanza di comprensione, disturbi fisici di lieve entità, etc.);
- **ALTO** = l'impatto è alto quando potranno esserci conseguenze significative che gli interessati dovrebbero riuscire a superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, perdita di posti di lavoro, danni alla proprietà, citazioni in giudizio, etc., peggioramento della salute);
- **MOLTO ALTO** = l'impatto è molto alto quando gli interessati potranno subire conseguenze significative o irreversibili che non saranno in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, etc.).

B. RISORSE TECNICHE – AREA RISORSE TECNICHE

N.	DOMANDE SU RISORSE TECNICHE	RISPOSTE	
		SI	**NO**

ASP IMMeS e PAT
Via Marostica 8, 20146 Milano Tel. 02.4029.1
E-mail *ufficio.protocollo@pioalbergotrivulzio.it*
PEC *ufficio.protocollo@pioalbergotrivulzio.legalmail.it*
Codice Fiscale/Partita IVA: 04137830966

1	Qualche parte del trattamento viene eseguita tramite internet? (Se si, aumentano le minacce esterne soprattutto se raggiungibili via web ed accessibile a tutti)		
2	Viene fornito l'accesso dall'esterno al sistema interno di trattamento dati tramite internet?		
3	Il sistema di trattamento è connesso con altro sistema o servizio it? (Se si posso nascere ulteriori minacce per difetti di sicurezza dei sistemi connessi ed eventuali altre persone non autorizzate)		
4	Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento? (Importanza dell'ambiente fisico di trattamento ed eventuali accessi da parte di risorse non autorizzate)		
5	Il sistema di trattamento è progettato e mantenuto senza seguire le migliori prassi (Progettazione, implementazione e manutenzione del sistema che possono comportare ulteriori rischi)		

IN CONLUSIONE: STABILIRE IN BASE ALLE RISPOSTE QUI SOPRA IL LIVELLO DI PROBABILITA' GENERALE DELLE MINACCE PER L'AREA RISORSE TENCICHE E DI RETE

Basso (1): è improbabile.
Medio (2): è ragionevole che si manifesti.
Alto (3): è probabile

C. AREA PROCESSI E PROCEDURE

N.	DOMANDE SU AREA PROCESSI E PROCEDURE	RISPOSTE	
		SI	NO
1	Ruoli e responsabilità sono vaghi e non chiaramente definiti? (il trattamento potrebbe diventare incontrollato con uso non autorizzato delle risorse e compromettere la sicurezza complessiva)		
2	L'uso della rete, del sistema e delle risorse non è chiaramente definito? (possono sorgere minacce a causa di incomprensioni o utilizzi impropri, una chiara definizione delle politiche può ridurre potenziali rischi)		
3	I dipendenti sono autorizzati a trasferire, archiviare o trattare dati personali al di fuori dei locali dell'organizzazione? (nascerebbero rischi aggiuntivi legati a canali di trasmissione insicuri e all'uso non autorizzato di queste informazioni)		
4	I dipendenti sono autorizzati a trasferire, archiviare o trattare dati personali al di fuori dei locali dell'organizzazione? (nascerebbero rischi aggiuntivi legati a canali di trasmissione insicuri e all'uso non autorizzato di queste informazioni)		

ASP IMMeS e PAT
Via Marostica 8, 20146 Milano Tel. 02.4029.1
E-mail *ufficio.protocollo@pioalbergotrivulzio.it*
PEC *ufficio.protocollo@pioalbergotrivulzio.legalmail.it*
Codice Fiscale/Partita IVA: 04137830966

5	Le attività di trattamento sono eseguite senza la creazione di file di registro? (la presenza di tali meccanismi diminuirebbe l'abuso intenzionale o accidentale di processi, procedure e risorse)		

IN CONCLUSIONE: STABILIRE IN BASE ALLE RISPOSTE QUI SOPRA IL LIVELLO DI PROBABILITA' GENERALE DELLE MINACCE PER L'AREA PROCESSI E PROCEDURE

Basso (1): è improbabile.
Medio (2): è ragionevole che si manifesti.
Alto (3): è probabile

D. AREA PARTI E PERSONE COINVOLTE

N.	DOMANDE SU AREA PARTI E PERSONE COINVOLTE	RISPOSTE	
		SI	NO
1	Il trattamento è eseguito da un numero indefinito di dipendenti? (aumentano le possibilità di abuso a causa del fattore umano, definire chi ne ha bisogno limitando l'accesso a loro contribuisce alla sicurezza del sistema)		
2	Qualche parte di trattamento è eseguita da una terza parte? (se sono presenti contraenti esterni possono essere introdotte altre minacce, vanno selezionati adeguatamente per offrire il massimo della sicurezza definendo quale parte del processo è loro assegnata e mantenendo un alto livello di controllo)		
3	Gli obblighi delle parti o persone coinvolte sono ambigui e non chiaramente definiti? (se i dipendenti non sono informati sui loro obblighi aumentano le minacce derivanti da un uso improprio accidentale come la divulgazione o la distruzione)		
4	Il personale coinvolto ha familiarità con il tema della sicurezza delle informazioni? (se i dipendenti non sono consapevoli della necessità di applicare le misure possono causare altre minacce, tramite una formazione adeguata è possibile sensibilizzarli sugli obblighi di protezione e sull'applicazione delle misure stabilite)		
5	Le persone/parti coinvolte trascurano l'archiviazione e/o la distruzione sicura dei dati? (Molte violazioni sono dovute a mancanza di misure di protezione fisica, particolare attenzione ai file cartacei anch'essi necessari di adeguata protezione da divulgazione o riutilizzo non autorizzato)		

E. AREA SETTORE E SCALA DEL TRATTAMENTO

N.	DOMANDE SU SETTORE E SCALA DEL TRATTAMENTO	RISPOSTE	
		SI	NO
1	Ritieni che il tuo settore di operatività sia esposto ad attacchi informatici? se si sono già verificati attacchi nello stesso settore del titolare è indicazione della necessità di adottare misure per evitare un evento simile		
2	Ci sono stati attacchi informatici all'organizzazione negli ultimi due anni?		

ASP IMMeS e PAT
Via Marostica 8, 20146 Milano Tel. 02.4029.1
E-mail *ufficio.protocollo@pioalbergotrivulzio.it*
PEC *ufficio.protocollo@pioalbergotrivulzio.legalmail.it*
Codice Fiscale/Partita IVA: 04137830966

	se ci sono già stati vanno prese ulteriori misure per evitarne altri		
3	Sono arrivate notifiche o reclami riguardo la sicurezza del sistema informatico nell'ultimo anno? Bug e vulnerabilità note vengono sfruttate per effettuare attacchi, vanno esaminate le comunicazioni in tal senso in modo che non influiscano sui sistemi in uso		
4	L'operazione di elaborazione riguarda un grande volume di individui e/o dati personali? tipologie e volume di dati (scala) possono rendere interessanti i dati per gli aggressori		
5	Esistono *best practice* di sicurezza specifiche per il settore in cui opera l'organizzazione che non sono state seguite? se presenti, solitamente sono adattate ai bisogni e rischi del settore, non seguirle è un indicatore di scarsa gestione della sicurezza		

IN CONCLUSIONE: STABILISCI IN BASE ALLE RISPOSTE QUI SOPRA IL LIVELLO DI PROBABILITA' GENERALE DELLE MINACCE PER L'AREA SETTORE E SCALA DEL TRATTAMENTO

Basso (1): è improbabile.
Medio (2): è ragionevole che si manifesti.
Alto (3): è probabile

ASP IMMeS e PAT
Via Marostica 8, 20146 Milano Tel. 02.4029.1
E-mail *ufficio.protocollo@pioalbergotrivulzio.it*
PEC *ufficio.protocollo@pioalbergotrivulzio.legalmail.it*
Codice Fiscale/Partita IVA: 04137830966