Atto di Nomina
Responsabile del Trattamento
(ai sensi dell'Articolo 28 del Regolamento UE 2016/679)

L'**Ospedale Pediatrico Bambino Gesù** (di seguito anche "**Ospedale**" o "**OPBG**") - Istituto di Ricovero e Cura a Carattere Scientifico, Istituzione della Santa Sede, con sede a Roma, Piazza S. Onofrio n. 4, in una delle zone extraterritoriali riconosciute dal Trattato Lateranense del 1929, Codice Fiscale 80403930581, in qualità di Titolare del trattamento ("**Titolare**") ed in persona di Tiziano Onesti, nella sua qualità di Presidente del Consiglio di Amministrazione e come tale dotato di idonei poteri,

preso atto che

- l'art. 4, comma 1, n. 7 del Regolamento UE 2016/679 (di seguito anche "RGPD" o "Regolamento") definisce «Titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- l'art. 4, comma 1, n. 8 del RGPD definisce «Responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- il presente accordo (di seguito "**Accordo**" o "**Nomina**") rappresenta l'atto giuridico di formalizzazione delle responsabilità come previsto dal paragrafo 3 del citato articolo 28 RGPD in relazione ai trattamenti definiti nell'Appendice 1 ed è allegato sostanziale del Contratto per la fornitura degli strumenti necessari per l'incremento del pacchetto strumentale già in dotazione all'Ospedale nell'ambito dell'iniziativa PNRR e la creazione di un Centro Nazionale per terapia RNA e Terapia Genica (di seguito anche "**Contratto**") stipulato tra le Parti;

NOMINA

Responsabile del trattamento ai sensi dell'articolo 28 (C81) del Regolamento UE 2016/679 la la Miltenyi Biotec s.r.l., in persona del legale rappresentante pro-tempore Dott. Stefan Gyorgi Otto Miltenyi, con sede legale in Bologna, 40133, Via Paolo Nanni Costa, 30, partita IVA 02077231203 (di seguito denominato "**Responsabile**").

La Nomina potrebbe essere oggetto di revisione/integrazione a seguito di specifica attività di verifica programmata dal Titolare con il supporto del Data Protection Officer ("**DPO**") designato dall'Ospedale.

1. ***Garanzie generali di sicurezza prestate dal Responsabile (Art. 28.1)***

Il Responsabile del trattamento garantisce la corretta applicazione delle misure di sicurezza di cui all'Appendice 2 della Nomina e di ogni altra misura adeguata che si dovesse rendere necessaria ex artt. 25 e 32 RGPD, tale da soddisfare, nella loro totalità, i requisiti posti dal Regolamento, dal D. Lgs. 196/2003 e dai provvedimenti del Garante per la Protezione dei dati Personali ("GPDP").

2. ***Autorizzazione nomina Sub-Responsabili (Art. 28.2 – 28.4)***

Ai sensi dell'art. 28.2 del Regolamento con la presente si fornisce espressa autorizzazione scritta generale alla individuazione da parte del Responsabile di altri soggetti che svolgano, per conto del Responsabile medesimo, il ruolo di "Sub-Responsabili". A fronte di tale autorizzazione, si richiede al Responsabile di comunicare alla scrivente l'elenco di tutti gli eventuali soggetti individuati in qualità di Sub-Responsabili. L'Ospedale provvederà a verificare eventuali profili di criticità emergenti dalle comunicazioni ricevute e si riserva la facoltà di limitare e/o revocare l'autorizzazione ivi concessa. Nel caso in cui nel tempo intervengano modifiche, aggiunte o sostituzioni dei Sub-Responsabili inizialmente comunicati, tali nuove nomine dovranno essere inoltrate alla scrivente al fine di effettuare le opportune valutazioni (anche in termini oppositivi) relativamente alla protezione dei dati personali.
Si precisa come è obbligo del Responsabile del trattamento individuare e nominare in forma scritta i propri Sub-Responsabili; tale atto di nomina/individuazione dovrà riproporre a carico del Sub-Responsabile i medesimi obblighi posti a carico del Responsabile e specificati nel presente documento, in particolare l'atto dovrà individuare le misure tecniche ed organizzative adeguate per garantire che il trattamento soddisfi i requisiti di sicurezza richiesti dal Regolamento.
Si evidenza come il Responsabile conservi nei confronti dell'Ospedale Pediatrico Bambino Gesù, Titolare del trattamento, ogni responsabilità derivante dall'eventuale inadempimento posto in essere dal Sub-Responsabile.

3. ***Prescrizioni poste a carico del Responsabile (art. 28.3)***

Per lo svolgimento delle attività di trattamento dati personali conseguenti al servizio affidato al Responsabile, lo stesso dovrà:

a) comunicare preventivamente l'eventuale trasmissione dei dati personali verso un Paese Terzo (non appartenente allo Spazio Economico Europeo); in tali casistiche il Titolare si riserva la facoltà di esprimere apposita autorizzazione alla trasmissione a meno che tale trasmissione non sia espressamente richiesta dell'Unione o dal diritto nazionale;

b) autorizzare espressamente al trattamento dei dati personali i propri dipendenti/collaboratori/soci/volontari attraverso modalità che garantiscano che tali soggetti siano obbligati al rispetto della riservatezza nei confronti dei dati che si troveranno a trattare in funzione del proprio incarico/ruolo;
c) garantire di aver effettuato una analisi dei rischi sui trattamenti oggetto della responsabilità e, ove necessario, una Valutazione d'impatto ai sensi dell'art. 35 del Regolamento; i documenti comprovanti l'analisi del rischio e l'eventuale valutazione di impatto dovranno essere messi a disposizione del Titolare del trattamento su richiesta di quest'ultimo;
d) garantire la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; le modalità per garantire tali livelli di sicurezza dovranno essere comunicate al Titolare nel caso di esplicita richiesta;
e) garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; le modalità per garantire tali livelli di sicurezza dovranno essere comunicate al Titolare nel caso di esplicita richiesta;
f) garantire la presenza di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; le modalità per garantire tali livelli di sicurezza dovranno essere comunicate al Titolare nel caso di esplicita richiesta (Appendice 2 del presente accordo);
g) garantire che tutti i soggetti che agiscono sotto l'autorità del Responsabile e che abbiano accesso ai dati non trattino tali dati se non sono stati istruiti in tal senso dal Responsabile stesso;
h) garantire il necessario apporto al Titolare del trattamento qualora nei confronti di questo vengano esercitati i diritti che il Regolamento (al capo III) riconosce agli interessati i quali impattino sui dati personali oggetto della presente nomina;
i) garantire la comunicazione al Titolare (ai sensi dell'art. 33.2 del Regolamento) di tutti gli eventi di violazione dei dati personali, entro 24 ore dall'evento, al fine di consentire al Titolare stesso il rispetto delle attività di notifica all'Autorità di controllo stabilite dall'articolo 33 del Regolamento. La comunicazione da parte del Responsabile al Titolare dovrà avvenire senza ingiustificato ritardo al seguente indirizzo mail dpo@opbg.net (Appendice 2 - Contatti) e dovrà contenere almeno i seguenti punti:
    - natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
    - il nome e i dati di contatto del Data Protection Officer o di altro punto di contatto presso cui ottenere più informazioni;
    - descrivere le probabili conseguenze della violazione dei dati personali;
    - descrivere le misure adottate da parte del responsabile del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti

negativi (il Responsabile sarà tenuto a mantenere presso i propri uffici la documentazione necessaria a descrivere le violazioni dei dati subite);

j) cancellare e/o restituire al Titolare tutti i dati personali una volta cessata l'erogazione dei servizi relativi al trattamento, cancellando anche le copie esistenti sui propri database, salvo che il diritto dell'Unione o degli stati membri preveda la conservazione dei dati; qualora al termine del servizio il Titolare non richieda espressamente la restituzione dei dati questi si intenderanno soggetti ad obbligo di cancellazione;
k) rendersi disponibile a sottoporsi ad attività di auditing da parte del Titolare del trattamento, o di un delegato di quest'ultimo, qualora questo ne ravvisasse la necessità;
l) comunicare al titolare del trattamento l'adesione ad eventuali codici di condotta di cui all'articolo 40 o ad un meccanismo di certificazione di cui all'articolo 42 del Regolamento;
m) attenersi ai criteri di durata del trattamento comunicati dal Titolare;
n) trasmettere una relazione - con cadenza annuale - al Titolare con un riepilogo delle attività effettuate in ottemperanza alla Nomina, avendo cura di indicare gli incidenti informatici e le violazioni dei dati personali avvenute.

4. ***Responsabilità***

Chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal Titolare o dal Responsabile. Il Responsabile risponde per il danno causato dal trattamento se non ha adempiuto gli obblighi posti dal Regolamento specificatamente diretti ai responsabili o ha agito in modo difforme o contrario rispetto alle legittime istruzioni impartite dal Titolare nel presente atto.
In caso di richieste di risarcimento pervenute al Titolare, per violazioni compiute dal Responsabile, il Titolare si riserva il diritto di rivalsa nei confronti del Responsabile stesso.
Per quanto riguarda le sanzioni imputabili da parte dell'Autorità Garante per la Protezione dei Dati Personali, fanno fede gli art. 82, 83 e 84 del Regolamento.
In caso di accertata violazione delle disposizioni del Regolamento o dell'Accordo, il Titolare si riserva il diritto di mettere in atto le misure ritenute corrette nei confronti del Responsabile.
Se la violazione si configurasse di particolare gravità è fatto salvo il diritto del Titolare di rescindere il Contratto.

5. <u>Durata, risoluzione e norme di rinvio</u>

In relazione alla durata, alla risoluzione, nonché a quanto non espressamente disposto nell'Accordo, si rinvia alle disposizioni contenute nel Contratto, di cui la Nomina costituisce allegato sostanziale.

_____, _____

Ospedale Pediatrico Bambino Gesù (Titolare del trattamento)
Tiziano Onesti

TIZIANO
ONESTI
06.10.2023
15:14:34
GMT+00:00

<u>Per accettazione</u>

Miltenyi Biotec S.r.l. (Responsabile del trattamento)
Dott. Stefan Gyorgi Otto Miltenyi

Firmato digitalmente da: STEFAN GYORGI OTTO MILTENYI
Data: 09/10/2023 11:10:25

Appendice 1

Categorie di interessati:
I Dati Personali riguardano: pazienti, dipendenti, collaboratori e comunque qualsivoglia soggetto che opera in nome e per conto di ciascuna Parte.

Tipo di Dati Personali oggetto di trattamento
I dati oggetto di trattamento appartengono:

- alla categoria di dati comuni: dati identificativi, anagrafici e di contatto;
- alla categoria dei dati particolari: dati relativi alla salute;

Natura e finalità del trattamento
Il trattamento dei dati personali viene effettuato per conto del Titolare del trattamento e in ragione dell'esecuzione delle finalità perseguite dallo stesso ossia: garantire la fornitura degli strumenti necessari per l'incremento del pacchetto strumentale già in dotazione all'Ospedale nell'ambito dell'iniziativa PNRR e la creazione di un Centro Nazionale per terapia RNA e Terapia Genica, giusto Contratto stipulato tra le Parti.
Il trattamento dei dati per le suddette finalità ha natura: Facoltativa, tuttavia necessaria per le finalità perseguite.

Durata del trattamento
Il trattamento sarà effettuato per tutta la durata del Contratto tra le Parti.

Modalità di Trattamento
In relazione alle indicate finalità, il trattamento dei dati personali avviene mediante: strumenti manuali e informatici.

Finanziato dall'Unione europea
NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

APPENDICE 2
(Misure organizzative e tecniche adottate dal Responsabile)

Indice

1. Descrizione delle misure di sicurezza tecniche ed organizzative 8
2. Amministratori di Sistema 8
3. Autenticazione 8
4. Salvaguardia dati e dispositivi 9
5. Autorizzazione 10
6. Difesa 10
7. Disponibilità dati 10
8. Protezione dati 11
9. Dispositivi rimovibili 11
10. Ruoli di sicurezza 11
11. Terze parti 11
12. Asset Management 12
13. Sicurezza fisica del Centro Elaborazione Dati ("CED") 12
14. Controllo degli accessi 12
15. Integrità dei sistemi 13
16. Vulnerability assessment e penetration testing 13
17. Gestione degli incidenti e delle violazioni 13
18. Business continuity e Disaster Recovery 14
19. Formazione 14
20. Registrazione delle operazioni 14
21. Sviluppo software e gestione ambienti 14
22. Change management 15
23. Rapporti di lavoro 15
24. Conformità 16

Contatti Ospedale Pediatrico Bambino Gesù 16

***

1. Descrizione delle misure di sicurezza tecniche ed organizzative

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a garantire un livello di sicurezza non inferiore a quello previsto dalle misure tecniche e organizzative di seguito descritte.

2. Amministratori di Sistema

Il Responsabile si impegna a rispettare il Provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008 (e sue successive modifiche) denominato "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"

2.1 Designazione

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere alla redazione di una lettera di designazione individuale per ogni amministratore di sistema, successivamente alla valutazione dell'esperienza, della capacità e dell'affidabilità dei soggetti, contenente l'elencazione analitica degli ambiti di operatività.

2.2 Revisione dell'operato degli Amministratori di Sistema

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere, con cadenza almeno annuale, a un processo di revisione dell'operato degli amministratori di sistema tramite i mezzi che riterranno adeguati.

2.3 Lista degli Amministratori di Sistema

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a produrre, su richiesta del Titolare, una lista del personale designato quale amministratore di sistema recante l'elenco delle funzioni ad esso attribuite.

2.4 Logging

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare un software di *operational intelligence* che produca dei *log* di accesso relativi ai sistemi su cui operano gli amministratori di sistema, aventi caratteristiche di completezza e inalterabilità nonché passibili di verifica di integrità e da conservare per almeno sei mesi.

3. Autenticazione

3.1 Credenziali

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere alla creazione di una *password* alfanumerica di almeno 8 caratteri in lunghezza, contenente maiuscole/minuscole e caratteri speciali. In alternativa, il Responsabile e gli eventuali Sub-Responsabili si impegnano a garantire il possesso di un *token* o, per trattamenti di particolare rilevanza in termini sia legali che di criticità per il core business aziendale del Titolare, la verifica di caratteristiche biometriche univoche e univocamente digitalizzabili come ad esempio l'impronta digitale. Il Responsabile e gli eventuali Sub-Responsabili si impegnano, eventualmente, su espressa richiesta del Titolare, a procedere alla combinazione di due o più fattori di autenticazione. Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad applicare i criteri summenzionati su tutti i sistemi e applicazioni aziendali.

3.2 Modifica periodica

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a forzare un cambio di *password* periodico automatizzato, che sia al più di 90 giorni. Il Responsabile e gli eventuali Sub-Responsabili si impegnano, inoltre, a forzare tecnicamente un cambio *password* al primo accesso per i nuovi utenti.

3.3 Credenziali individuali

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a non assegnare credenziali condivise ma di assegnare unicamente credenziali individuali, in particolar modo per quanto riguarda le figure dotate di permessi elevati su sistemi e applicazioni.

3.4 Segnalazione inattività

Il Responsabile e gli eventuali Sub-Responsabili si impegnano affinché tutte le credenziali, eccetto quelle utilizzate per soli scopi di gestione tecnica, quali utenze macchina o credenziali di root, vengano segnalate come inattive dopo sei mesi.

3.5 Disattivazione o modifica credenziali

Il Responsabile e gli eventuali Sub-Responsabili si impegnano affinché tutte le credenziali, eccetto quelle utilizzate per soli scopi di gestione tecnica, scadano automaticamente al più dopo sei mesi o siano aggiornate relativamente al cambio di mansione dell'incaricato.

3.6 *Non disclosure*

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare e documentare opportune procedure per accedere ai dati in caso di assenza prolungata dell'incaricato che li detiene. Tali procedure non dovrebbero in alcun caso prevedere la *disclosure* della *password* dell'incaricato.

4. Salvaguardia dati e dispositivi

4.1 Protezione delle credenziali

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a redigere una *policy* contenente delle chiare istruzioni circa le cautele da adottare per assicurare la segretezza delle credenziali e la diligente custodia dei dispositivi assegnati.

4.2 Protezione da danni e furti

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a redigere una *policy* contenente delle chiare istruzioni circa le cautele da adottare per assicurare la salvaguardia dei dispositivi assegnati.

4.3 Protezione delle sessioni

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere ad implementare un sistema di *lock screen/screensaver* con reinserimento delle credenziali ogni qualvolta non vi è fisicamente un incaricato presente a presidiare/utilizzare la postazione di lavoro. Tale *lock screen* dovrebbe essere impostato affinché si attivi in automatico dopo meno di 5 minuti di inattività.

5. Autorizzazione

5.1 Esistenza profili autorizzativi

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare un sistema centralizzato per la gestione di autenticazione e autorizzazione. Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere ad un censimento dei permessi effettivamente da attribuire, prima di procedere con la loro assegnazione.

5.2 Minimizzazione dei permessi

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere in via residuale, non assegnando più permessi del dovuto e tenendo a mente i principi del *least privilege* e del *need to know* ossia consentendo la visualizzazione dei soli dati necessari a svolgere la funzione lavorativa, con attribuzione dei permessi minimi su sistemi e applicativi.

5.3 Revisione profili

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a verificare la coerenza e la presenza dei profili autorizzativi almeno annualmente, e di procedere alla verbalizzazione di tale attività.

6. Difesa

6.1 Aggiornamenti

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a monitorare e gestire in maniera centralizzata e/o automatizzata gli aggiornamenti, o ad adottare idonei mezzi organizzativi in maniera tale da rendere le macchine e le applicazioni costantemente aggiornate tenendo in particolare considerazione gli aggiornamenti di sicurezza.

6.2 Isolamento sistemi non più supportati

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a segregare le macchine che per ragioni di operatività vengono ancora utilizzate nonostante non siano più supportate da aggiornamenti.

6.3 *Data protection by design*

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a formalizzare o adottare delle linee guida di *data protection by design*, assicurandosi che i sistemi aziendali sviluppati internamente siano coerenti con esse.

6.4 Programmi di protezione allo stato dell'arte

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare e mantenere aggiornati i *software* di protezione quali antivirus, la cui gestione dovrebbe avvenire in maniera preferibilmente centralizzata, *firewall*, contenente preferibilmente moduli IDS e IPS, *antispam*.

7. Disponibilità dati

7.1 *Backup*

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a implementare un sistema di *backup*, formalizzando un piano di *backup*, documentando le tecnologie in atto all'interno di una *policy* contenente altresì una procedura per eseguire correttamente tale attività.

7.2 Piani di ripristino

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere ad effettuare test di ripristino, verbalizzare i test effettuati e le procedure di ripristino, documentando, inoltre, i tempi necessari per eseguirle.

8. Protezione dati

8.1 Cifratura e confinamento

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare tecniche di cifratura a tutti i livelli: *full disk encryption* sulle unità di massa, *transparent data encryption* sui *database*, *file-level encryption* per file contenenti credenziali, tramite l'utilizzo di standard crittografici non deprecati.

8.2 Pseudonimizzazione

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere alla pseudonimizzazione dei dati personali eventualmente presenti all'interno dei *database*.

8.3 Cifratura in transito

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare e documentare le tecnologie di cifratura in transito.

9. Dispositivi rimovibili

9.1 Dispositivi rimovibili

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a regolamentare l'utilizzo dei supporti rimovibili e la loro protezione.

9.2 Sanitizzazione dei dispositivi rimovibili

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a formalizzare opportune procedure per la distruzione, cifratura e/o formattazione dei dispositivi rimovibili e dei dispositivi aziendali in uso.

10. Ruoli di sicurezza

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a definire la funzione aziendale che sia responsabile per la *cybersecurity*, ossia chi possa ricoprirla in azienda con le relative responsabilità. Ciò può comportare di designare un CISO (*Chief Information Security Officer*) o, più generalmente, un CSO (*Chief Security Officer*) o, generalmente, una figura che abbia l'autorità, in azienda, di perimetrare, sotto il piano della sicurezza, informatica e delle informazioni, i processi dell'organizzazione. Tale figura dovrebbe essere reperibile al fine di riscontrare eventuali incidenti di sicurezza e dovrebbe essere nota a tutti i dipendenti.

11. Terze parti

11.1 Contratti

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a redigere tutti i contratti rilevanti con gli outsourcer e con i fornitori in maniera tale che includano anche i requisiti di sicurezza pertinenti al servizio o prodotto fornito.

11.2 Audit di secondo livello

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a verificare periodicamente la coerenza con i requisiti di sicurezza contrattualizzati tramite audit di secondo livello opportunamente contrattualizzati e calendarizzati.

12. Asset Management

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a rimuovere *asset* e credenziali degli impiegati non più in forze all'interno dell'infrastruttura del Responsabile e Sub-Responsabile, o che abbiano cambiato mansione e asset necessari per svolgere la mansione.

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad effettuare una verifica periodica dell'effettiva rimozione di asset e credenziali.

13. Sicurezza fisica del Centro Elaborazione Dati ("CED")

13.1 Misure di sicurezza fisica

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a redigere e implementare procedure formali di accesso per consentire l'accesso fisico al CED. I server e le macchine sulle quali sono conservati i dati del Titolare, all'interno del CED, sono ospitati in strutture che richiedono l'accesso con chiave dotata di scheda elettronica, con allarmi collegati ad eventuali SOC o centri di monitoraggio della sicurezza fisica. Le richieste di accesso alle chiavi dotate di schede elettroniche devono essere sottoposte ad un processo formalizzato di approvazione.

13.2 Visitatori

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad autenticare i visitatori prima dell'accesso al CED. Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad accompagnare all'interno della struttura del CED i visitatori e di predisporre un registro di accesso degli stessi. Al fine accedere all'infrastruttura del CED, i visitatori dovranno (i) ottenere in anticipo l'approvazione da parte dei responsabili del CED per le aree interne che desiderano visitare; (ii) accedere tramite identificazione in loco.

13.3 Condizioni del CED

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a monitorare costantemente le condizioni del CED, considerando le variabili relative, tra le altre, a temperatura, condizione dell'impianto di raffreddamento, polvere, umidità e a verificare periodicamente il funzionamento dei sensori.

14. Controllo degli accessi

14.1 Credenziali individuali

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a creare credenziali individuali per ciascun incaricato e istruire gli stessi incaricati circa la necessità di non condividere le credenziali.

14.2 Presenza di profili autorizzativi

Il Responsabile e gli eventuali Sub-Responsabili si impegnano, nei limiti di quanto consentito dai sistemi, a creare dei profili autorizzativi ai quali assegnare le utenze create.

Finanziato dall'Unione europea
NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani

14.3 Network access control

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a valutare la possibile introduzione di una soluzione per il NAC (*Network Access Control*) allo scopo di autenticare le macchine sulla rete.

14.4 Separazione VLAN

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a prendere in considerazione la possibilità di segmentare la rete in VLAN separate.

14.5 Sessioni concorrenti

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a impostare un numero massimo di sessioni concorrenti sui sistemi per lo stesso utente.

14.6 *Rate limiting*

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a impostare un numero massimo di tentativi falliti di login prima del blocco dell'account su tutti i sistemi e applicativi aziendali.

15. Integrità dei sistemi

15.1 *SQL Injection*

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad attenzionare e implementare processi di sanitizzazione degli input al fine di scongiurare attacchi noti quali SQL Injection.

15.2 Gestione password e chiavi di cifratura

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare soluzioni per la gestione di password e chiavi di cifratura.

15.3 Assenza di possibile disattivazione

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a non consentire agli incaricati, non preposti a funzioni di sicurezza, di poter disattivare le misure di protezione sulle loro macchine.

16. Vulnerability assessment e penetration testing

16.1 Periodicità

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a condurre sessioni di *vulnerability assessment* e *penetration testing* sui sistemi aziendali con periodicità almeno annuale.

16.2 Automatizzazione

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad impiegare dei tool per il *Vulnerability Assessment* automatizzato, che tuttavia non deve sostituire quello tradizionale.

17. Gestione degli incidenti e delle violazioni

17.1 Procedure di *incident handling*

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a introdurre prassi, protocolli e procedure relative all'*incident handling* e gestire tutti gli eventi di sicurezza e/o gli incidenti di sicurezza tramite una procedura formalizzata con dei ruoli prestabiliti.

Finanziato dall'Unione europea
NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani

17.2 Formazione del personale

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a rendere edotto il personale relativamente alle procedure di *incident handling*.

17.3 *Alert*

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a prendere in considerazione, se ritenuto funzionale e adeguato al rischio, ad adottare un SIEM, o soluzioni alternative che raggiungano lo scopo di segnalare anomalie e/o attacchi in corso.

17.4 Registro degli incidenti

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a stilare e mantenere un registro degli incidenti, che contenga almeno le informazioni in merito a scoperta, analisi, contenimento, mitigazione e recupero dai vari incidenti di sicurezza.

17.5 Comunicazione al titolare

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a comunicare tempestivamente, nell'arco di 24 ore dalla scoperta, gli incidenti di sicurezza occorsi sulle loro infrastrutture al Titolare.

18. Business continuity e Disaster Recovery

18.1 *Business continuity*

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a garantire la continuità operativa per tutti i servizi offerti al Titolare, tramite, se del caso, la formalizzazione di un *Business Continuity Plan*.

18.2 *Disaster recovery*

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a rendere possibile il ripristinare tutti i dati del Titolare in seguito a disastri, tramite, se del caso, la formalizzazione di una strategia per il *Disaster Recovery*, includendo *policy* dettagliate per la conservazione sicura delle copie di *backup* e loro ripristino.

18.3 Cifratura e custodia

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a prevedere la cifratura del *backup* e di prevedere procedure sicure per la loro custodia.

19. Formazione

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a formalizzare training periodici di *security awareness* per tutto il personale d'ufficio, al fine di ridurre l'eventualità di intrusioni, riuscita di *phishing* o infezione da malware.

20. Registrazione delle operazioni

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare un *software* di *operational intelligence* che produca log inalterabili, completi e passibili di verifica d'integrità che operi sui sistemi sui quali sono trattati i dati personali riferibili al Titolare.

21. Sviluppo software e gestione ambienti

21.1 Linee guida sviluppo

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare e adottare linee guida di scrittura del codice sicuro.

21.2 Separazione ambienti

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a separare gli ambienti di *test*, sviluppo e produzione.

21.3 Formalizzazione dei processi di produzione

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a formalizzare le procedure necessarie al passaggio dall'ambiente di *test* all'ambiente di produzione.

21.4 Testing

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a testare *software* e sistemi previo inserimento in produzione.

21.5 Patch

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a effettuare installazione e disinstallazione delle patch tramite prassi note.

21.6 Protezione dei dati di test

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a proteggere i dati di test tramite offuscamento o cifratura e di rendere gli stessi utilizzabili sono a personale autorizzato.

22. Change management

22.1 Formalizzazione del change management

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad effettuare cambiamenti ai sistemi critici tramite prassi note o procedure formalizzate.

22.2 Notifica al Titolare

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a notificare il Titolare in merito a notevoli cambiamenti relativi alla *User Experience*.

23. Rapporti di lavoro

23.1 Prima dell'instaurazione del rapporto di lavoro

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a prendere in considerazione le responsabilità della sicurezza delle informazioni durante l'assunzione di dipendenti, collaboratori e personale temporaneo (ad esempio attraverso adeguate descrizioni sulle mansioni da svolgere, controlli pre-assunzione) e ad inserirle all'interno dei contratti (ad esempio con termini e condizioni del rapporto di lavoro e sottoscrizione di ulteriori accordi volti a definire ruoli e responsabilità in tema di sicurezza, obblighi di conformità, ecc.).

23.2 Durante il rapporto di lavoro

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a garantire che i manager si assicurino che i dipendenti e i collaboratori siano consapevoli e motivati a rispettare i loro obblighi per garantire la sicurezza delle informazioni.

23.3 Conclusione o modifiche al rapporto di lavoro

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a gestire gli aspetti relativi alla sicurezza al momento dell'uscita di una persona dall'organizzazione, o nelle ipotesi di modifiche significative al ruolo ricoperto, come la restituzione delle informazioni e delle apparecchiature aziendali in possesso del soggetto uscente, l'aggiornamento dei permessi di

accesso, nonché il rispetto dei perduranti obblighi relativi alle informazioni riservate ed ai diritti di proprietà intellettuale, ai termini contrattuali, ecc. ed anche ai doveri etici.

24. Conformità

24.1 Conformità ai requisiti legali e contrattuali

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a garantire che l'organizzazione identifichi e documenti i suoi obblighi alle autorità esterne e ad altre terze parti in relazione alla sicurezza delle informazioni, compresa la proprietà intellettuale, la documentazione contabile, le informazioni relative alla *privacy* comunque idonee a consentire l'identificazione personale e la crittografia.

24.2 Revisione della sicurezza delle informazioni

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a garantire che i progetti dell'organizzazione relativamente alla sicurezza delle informazioni siano revisionati (verificati tramite *audit*) con modalità tali da garantire l'indipendenza della valutazione e rendicontate alla Direzione. Il Responsabile e gli eventuali Sub-Responsabili si impegnano altresì a garantire che i manager revisionino periodicamente la conformità dei dipendenti e dei sistemi alle *policy* di sicurezza, alle procedure, ecc., e promuovano azioni correttive ove necessario.

***

Contatti Ospedale Pediatrico Bambino Gesù

Titolare del trattamento: Ospedale Pediatrico Bambino Gesù - Piazza S. Onofrio n. 4 (Roma) – Tel. 06.6859.1 - E-mail: presidenza@opbg.net - PEC: presidenza@pec.opbg.net
Funzione Privacy OPBG: privacy@opbg.net
Data Protection Officer: Angelo Loiacono - Piazza S. Onofrio n. 4 (Roma) – Tel. 06.6859.4018 -E-mail: dpo@opbg.net – Pec: dpo@pec.opbg.net