***Prot. n.XXXXX del gg/mm/aaaaa***

***Rep. N.XXXX/aaaa***

***Oggetto:*** *Nomina a Responsabile Esterno del Politecnico di Milano per il contratto relativo alla FORNITURA DEL SERVIZIO SOSTITUTIVO DI MENSA MEDIANTE BUONI PASTO ELETTRONICI PER STUDENTI ASSEGNATARI DI BENEFICI DEL DIRITTO ALLO STUDIO – CIG ………………………..*

Preso atto che … ha la propria sede in … e che …

Considerati anche gli accordi e le convenzioni stipulate fra … e … e tenuto conto delle disposizioni di cui al D. Lgs. 196/2003 – Codice in materia di protezione dei dati personali e al Regolamento (UE) 2016/679 – Regolamento generale sulla protezione dei dati personali,

Considerato che il Politecnico di Milano offre idonea garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, … , in qualità di titolare del trattamento

nomina

Politecnico di Milano, ai sensi e per gli effetti dell'art. 28 del Regolamento (UE) 2016/679, “**Responsabile del trattamento dei dati personali**” per i trattamenti nell’Allegato 1.

I trattamenti dovranno essere effettuati nell’ambito delle finalità e dei compiti affidati al responsabile esterno, secondo modalità connesse a tale scopo.

Il trattamento dei dati dovrà limitarsi alle operazioni strettamente necessarie per assicurare il conseguimento delle finalità stabilite nell’Allegato 1.

Il Politecnico di Milano dovrà adottare tutte le misure di sicurezza idonee a preservare i dati trattati da perdite, danneggiamenti e accessi non autorizzati, limitatamente ai poteri e doveri conferiti a seguito dei rapporti in essere.

I dati saranno trattati soltanto da soggetti specificatamente autorizzati dal Politecnico di Milano che dovranno utilizzarli in esecuzione delle prestazioni in oggetto e come definite nell’Allegato 1. Il Politecnico garantisce che tali soggetti sono impegnati alla riservatezza e/o sussiste un adeguato obbligo legale di riservatezza. Il Politecnico di Milano si impegna a fornire tutte le istruzioni necessarie alla corretta gestione dei dati personali. Il personale dipendente o i collaboratori che saranno autorizzati a svolgere le prestazioni in oggetto dovranno assicurare la massima serietà e affidabilità.

Si rappresenta inoltre l’obbligo per il Politecnico di Milano di impegnarsi a formare il personale interno alla propria struttura, così da renderlo edotto circa i principi di riservatezza imposti dal Regolamento (UE) 2016/679, fornendo istruzioni idonee per trattare i dati nell’ambito delle mansioni assegnate, monitorando il corretto adempimento delle istruzioni impartite.

Si rappresenta altresì l’obbligo per il Politecnico di Milano di impegnarsi, e impegnare i soggetti autorizzati, a quanto segue:

* trattare i dati personali conosciuti anche indirettamente e/o incidentalmente in virtù dell’esecuzione degli obblighi scaturenti da accordi e convenzioni in essere, nel rispetto dei principi di cui agli artt. 5 e seguenti del Regolamento (UE) 2016/679;
* trattare i dati personali secondo le istruzioni impartite dal titolare e esclusivamente per le finalità previste da accordi e convenzioni in essere;
* adottare tutte le misure idonee a tutelare i dati personali oggetto del trattamento nel rispetto del D. Lgs. 196/2003 e del Regolamento (UE) 2016/679 (Capo IV);
* rispettare quanto previsto dal Regolamento (UE) 2016/679 non solo in tema di misure di sicurezza, ma anche in relazione ai principi generali in esso stabiliti. Il Responsabile del trattamento adotta misure tecniche ed organizzative adeguate nelle operazioni di trattamento, prevedendo l’adozione delle misure previste dalla Circolare n. 2 del 18 aprile 2017 recante “Misure minime di sicurezza ICT per le pubbliche amministrazioni”, così come illustrato nell’Allegato 2, garantendone la implementazione e l’applicazione nei confronti del Titolare del trattamento;
* il Responsabile del trattamento in ottemperanza al proprio modello organizzativo privacy del Politecnico di Milano adottato con Decreto Direttore Generale n. 7229 del 20 ottobre 2020 recante “Modifiche apportate al Modello organizzativo privacy del Politecnico di Milano”; e in conformità al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”, così come modificato dal Provvedimento del Garante del 25 giugno 2009, e ad ogni altro pertinente provvedimento dell’Autorità ha valutato di nominare per i suoi servizi di ICT gli amministratori di sistema, che svolgeranno questo ruolo nell’ambito dei servizi messi a disposizione al Titolare;
* per quanto concerne i servizi di posta elettronica e di internet, … adotta le stesse prescrizioni previste specificatamente per tali servizi dal “Regolamento del Politecnico di Milano in materia di protezione dei dati personali e della sicurezza ICT” adottato con Decreto del Rettore, Rep. n. 6761 del 06.10.2020 e le relative “Istruzioni operative per il trattamento dei dati personali” adottate con Decreto del Direttore Generale, Rep. n. 7230 del 20.10.2020, disponibili al link: [www.normativa.polimi.it](http://www.normativa.polimi.it).
* i dati personali conosciuti non dovranno essere diffusi o trasmessi a terzi salvo i casi in cui, con l’autorizzazione scritta e secondo le indicazioni dell’Ateneo ciò sia necessario all’esecuzione dei trattamenti previsti dal contratto;
* il Responsabile si impegna altresì a comunicare tempestivamente al Titolare eventuali criticità riscontrate in merito alla sicurezza dei dati, così da renderlo edotto circa eventuali rischi in merito alla sicurezza dei dati trattati;
* nel caso in cui il Responsabile, anche per il tramite delle persone autorizzate, riceva istanze di accesso ex art. 15 Regolamento (UE) 2016/679 o altre istanze dall’interessato, si impegna a comunicarle tempestivamente per iscritto e comunque non oltre un giorno dalla ricezione, coadiuvandolo, ove necessario, a fornire un riscontro nei termini di legge;
* il Responsabile si impegna ad assistere il Titolare in caso di audit
* il Responsabile, su richiesta del Titolare, si impegna a collaborare nell’ambito di eventuali procedimenti che dovessero intervenire dinnanzi all’Autorità Garante o all’Autorità Giudiziaria, mettendo a disposizione elementi documentali e probatori rientranti nella sua sfera di competenza;
* secondo le indicazioni del Titolare, alla conclusione dei rapporti contrattuali in essere. Il Responsabile si impegna a distruggere e/o restituire e/o cancellare tutti i dati trattati per conto del Titolare, siano essi detenuti in formato cartaceo oppure informatico, e ciò senza pregiudizio alcuno per il Titolare o per gli interessati cui i dati si riferiscono. Si chiarisce che, anche alla scadenza del contratto, restano in vigore gli impegni di riservatezza e di segretezza dei dati in parola;
* qualora il Responsabile, in considerazione delle modalità di esecuzione del servizio e previa autorizzazione scritta del Titolare, ricorra ad altro Responsabile dovrà formalizzarne la nomina imponendogli il rispetto degli stessi oneri cui il medesimo si assume con il vincolo della presente nomina;
* il Responsabile è fin d'ora reso edotto che la violazione degli obblighi normativi in materia di tutela dei dati personali può comportare conseguenze civili e penali;
* si impegna a comunicare tempestivamente eventuali *data breach* all’indirizzo mail [mmaggi@maggilegal.it](mailto:mmaggi@maggilegal.it) e michela.maggi@milano.pecavvocati.it nel più breve tempo possibile e, in ogni caso, non oltre 24 ore dalla scoperta. La comunicazione dovrà indicare ogni elemento utile a contestualizzare il data breach quali: tipo di data breach, dati coinvolti e loro tipologia (compreso il loro livello di protezione), interessati coinvolti, potenziali danni per gli interessati, etc.

… , in quanto titolare del trattamento dei dati, potrà, come previsto dal Regolamento (UE) 2016/679, esercitare vigilanza e controllo sulla puntuale osservanza delle istruzioni impartite e delle vigenti disposizioni in materia di trattamento dei dati personali da parte del Responsabile. La verifica tramite richiesta di idonea documentazione attestante la conformità alla normativa sulla protezione dei dati personali ed eventuale altra documentazione occorrente per dimostrare l’ottemperanza agli obblighi di legge nei confronti delle autorità o di terzi.

Resta inteso che la nomina del Politecnico di Milano a Responsabile esterno decadrà in qualunque caso di cessazione di contratti e convenzioni in essere per la gestione del servizio in oggetto, con effetto dalla data di tale cessazione.

|  |  |
| --- | --- |
| …  Titolare del trattamento  ------------------------------------------- | Politecnico di Milano  Responsabile del trattamento    --------------------------------------------- |

***ALLEGATO 1***

***DESCRIZIONE DEL TRATTAMENTO***

|  |  |
| --- | --- |
| **FINALITÀ DEL TRATTAMENTO**  (*Inserire una descrizione del servizio che sottende il trattamento dei dati personali*) |  |
| **DATI PERSONALI OGGETTO DEL TRATTAMENTO**  *(Barrare le tipologie di dati trattati o inserire eventuali dati non indicati)* | ❑ personali comuni (sesso, anno di nascita, età, nazionalità) ❑ dati economici (es. codice iban)  ❑ immagini ❑ video ❑ dati relativi alla salute ❑ alla vita sessuale ❑ all'orientamento sessuale della persona ❑ dati genetici ❑ dati biometrici (es. riconoscimento facciale, impronta digitale etc.) ❑ dati personali che rivelano l'origine razziale o etnica ❑ opinioni politiche ❑ convinzioni religiose o filosofiche ❑ l'appartenenza sindacale ❑ dati giudiziari  ❑ ALTRO: Recapito telefonico, traffico telefonico, log di sistema |
| **CATEGORIE DI INTERESSATI**  *(Barrare i soggetti a cui si riferiscono i dati personali trattati)* | ❑ studenti ❑ personale docente ❑ personale tecnico amministrativo ❑ laureandi ❑ collaboratori ❑dottorandi ❑specializzandi ❑ fornitori ❑ tirocinanti ❑ visitatori ❑ soggetti esterni ❑ cittadini  ❑ ALTRO Personale e collaboratori di “…”. |
| **OPERAZIONI DI TRATTAMENTO**  (*Barrare le tipologie di trattamento dei dati o inserire eventuali trattamenti non indicati*) | ❑ consultazione ❑ uso ❑ comunicazione mediante trasmissione  ❑ diffusione o qualsiasi altra forma di messa a disposizione  ❑ conservazione ❑ raccolta ❑ registrazione ❑ estrazione  ❑ organizzazione ❑ strutturazione ❑ modifica ❑ adattamento  ❑ raffronto o l'interconnessione ❑ cancellazione ❑ distruzione  ❑ limitazione  ALTRO: …………………………………………………………………… |
| **PROCESSI AUTOMATIZZATI** | ❑ SI  ❑ NO |

***ALLEGATO 2***

***MISURE MINIME DI SICUREZZA***

|  |  |  |
| --- | --- | --- |
| **ABSC\_ID #** | **Descrizione** | **FNSC** |
| 1.1.1 | Implementare un inventario delle risorse attive correlato a quello ABSC 1.4 | ID.AM-1 |
| 1.3.1 | Aggiornare l’inventario quando nuovi dispositivi approvati vengono collegati in rete | ID.AM-1 |
| 1.4.1 | Gestire l’inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l’indirizzo IP | ID.AM-1 |
| 2.1.1 | Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l’installazione di software non compreso nell’elenco. | ID.AM-2 |
| 2.3.1 | Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato. | ID.AM-2 |
| 3.2.1 | Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall’organizzazione. | PR.IP-1 |
| 3.2.2 | Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard. | PR.IP-2 RC.RP-1 |
| 3.3.1 | Le immagini d’installazione devono essere memorizzate offline. | PR.IP-2 |
| 3.4.1 | Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri). | PR.AC-3 PR.MA-2 |
| 4.1.1 | Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche. | ID.RA-1 DE.CM-8 |
| 4.4.1 | Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza. | DE.CM-8 |
| 4.5.1 | Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni. | PR.MA-1 |
| 4.5.2 | Assicurare l’aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità. | PR.MA-1 |
| 4.7.1 | Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio. | PR.IP-12 RS.MI-3 |
| 4.8.1 | Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.). | ID.RA-4 ID.RA-5 PR-IP.12 |
| 4.8.2 | Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche. | PR.IP-12 |
| 5.1.1 | Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi. | PR.AC-4 PR.PT-3 |
| 5.1.2 | Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato. | PR.AC-4 PR.PT-3 |
| 5.2.1 | Mantenere l’inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata. | ID.AM-6 PR.AT-2 DE.CM-3 |
| 5.3.1 | Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell’amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso. | PR.IP-1 |
| 5.7.1 | Quando l’autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri). | PR.AC-1 PR.AT-2 |
| 5.7.3 | Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging). | PR.AC-1 PR.AT-2 |
| 5.7.4 | Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history). | PR.AC-1 |
| 5.10.1 | Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse. | ID.AM-6 |
| 5.10.2 | Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona. | ID.AM-6 |
| 5.10.3 | Le utenze amministrative anonime, quali “root” di UNIX o “Administrator” di Windows debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l’imputabilità di chi ne fa uso. | ID.AM-6 PR.AT-2 |
| 5.11.1 | Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza. | PR.AC-1 PR.AT-2 |
| 5.11.2 | Se per l’autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette. | PR.AC-1 PR.AT-2 |
| 8.1.1 | Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l’esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico. | DE.CM-4 DE.CM-5 |
| 8.1.2 | Installare su tutti i dispositivi firewall ed IPS personali. | DE.CM-1 |
| 8.3.1 | Limitare l’uso di dispositivi esterni a quelli necessari per le attività aziendali. | PR.PT-3 DE.CM-7 |
| 8.7.1 | Disattivare l’esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili. | PR.PT-2 |
| 8.7.2 | Disattivare l’esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file. | PR.AT-1 DE.CM-4 |
| 8.7.3 | Disattivare l’apertura automatica dei messaggi di posta elettronica. | PR.AT-1 DE.CM-4 |
| 8.7.4 | Disattivare l’anteprima automatica dei contenuti dei file. | PR.AT-1 DE.CM-4 |
| 8.8.1 | Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione. | PR.PT-2 DE.CM-4 |
| 8.9.1 | Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l’impiego di strumenti antispam. | DE.CM-1 DE.CM-4 |
| 8.9.2 | Filtrare il contenuto del traffico web. | DE.CM-1 DE.CM-4 |
| 8.9.3 | Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l’organizzazione ed è potenzialmente pericolosa (e.g. .cab). | DE.CM-1 DE.CM-4 |
| 10.1.1 | Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema. | PR.IP-4 |
| 10.3.1 | Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud. | PR.DS-6 |
| 10.4.1 | Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza. | PR.AC-2 PR.IP-4 PR.IP-5 PR.IP-9 |
| 13.1.1 | Effettuare un’analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica | ID.AM-5 |
| 13.8.1 | Bloccare il traffico da e verso url presenti in una blacklist. | ID.-AM3 PR.DS-5 DE.CM-1 |

***MISURE MINIME DI SICUREZZA FISICHE ADOTTATE PER LA FONDAZIONE***

Il Politecnico di Milano adotta un controllo accessi fisico ai propri spazi basati su un sistema di badge, finalizzato a salvaguardia e a tutela del patrimonio, e per impedire un accesso a persone prive di autorizzazione.

Ogni badge è collegato a un account Fondazione del Politecnico, che a sua volta è collegato a un individuo. Questo dispositivo consente di identificare tutte le persone presenti nelle strutture.

Il Responsabile ha adottato le seguenti misure di sicurezza:

* Accesso sicuro agli spazi della fondazione mediante lettori di badge;
* Accesso limitato a persone autorizzate in possesso di chiavi e/o schede elettroniche di accesso;
* Accesso solo a persone autorizzate e/o invitate dal titolare;
* Sistema di allarme di sicurezza o altre misure di sicurezza appropriate a tutela del patrimonio.