

Allegato A1: Requisiti non funzionali minimi inderogabili del sistema

Sommario

1.	Requisiti generali degli applicativi.....	2
2.	Modalità di erogazione dei servizi applicativi	2
3.	Trattamento dei dati personali.....	2
4.	Misure Minime di Sicurezza ICT.....	3
5.	Dislocazione dei datacenter.....	3
6.	Business continuity e disaster recovery	3
7.	Log degli accessi.....	4
8.	Ambiente di test	4
9.	Base di dati	4
10.	Autenticazione ed autorizzazione degli utenti e degli operatori per l'accesso ai servizi.....	4
11.	Integrazione con altri sistemi.....	5
12.	Domain dei server e indirizzi mail utilizzati per le comunicazioni agli utenti	5
13.	Migrazione storico dati pregressi.....	5
14.	Transitorio di passaggio ai nuovi servizi	5
15.	Formazione ed affiancamento.....	5
16.	Documentazione	6
17.	– Servizi di assistenza e manutenzione	6
a.	Manutenzione correttiva	6
b.	Manutenzione adeguativa	8
c.	Manutenzione ordinaria	8
d.	Manutenzione per adeguamenti normativi.....	8
18.	Supporto al termine del contratto.....	8
19.	Supporto in caso di cessazione del contratto	8
20.	Attività di Audit.....	8

L'Appaltatore nella Relazione Tecnica fornisca una descrizione dettagliata delle seguenti funzionalità obbligatorie del sistema, corredandole con videate e rendendo disponibile un ambiente demo, qualora sia utile per una migliore comprensione, al fine di fornire elementi utili alla valutazione.

1. Requisiti generali degli applicativi

Tutti gli applicativi dovranno essere resi disponibili esclusivamente mediante interfaccia Web. Il Fornitore dovrà dichiarare e garantire la compatibilità certificata degli applicativi con i browser più diffusi (Chrome, Safari, FireFox, Edge) garantendo l'aggiornamento alle successive evoluzioni.

L'interfaccia Web dovrà:

- essere "responsive", ovvero il layout e l'interfaccia dovranno adattarsi al dispositivo con cui si effettua l'accesso ai servizi
- essere disponibile per tutte le piattaforme mobile (smartphone e tablet con sistemi operativi Android e iOS)
- essere accessibile: l'interfaccia utente unificata dovrà essere conforme alla L. 4/2004, recante Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici. Inoltre, deve essere conforme ai requisiti tecnici previsti dalle "Linee Guida sull'accessibilità degli strumenti informatici" emanate dall'Agenzia per l'Italia Digitale (release del 21 dicembre 2022 [Linee guida sull'accessibilità degli strumenti informatici \(agid.gov.it\)](https://www.agid.gov.it/linee-guida))
- essere predisposta per il multilinguismo e avere una interfaccia front-office per gli utenti finali e una interfaccia back-office per gli operatori almeno bilingue (Italiano ed Inglese).

2. Modalità di erogazione dei servizi applicativi

Tutti gli applicativi dovranno essere resi disponibili in modalità Software as a Service (SaaS) e non richiedere l'installazione di componenti sw presso i datacenter del Committente. Tale servizio SaaS dovrà risultare qualificato da ACN e pubblicato nel Cloud MarketPlace ACN consultabile al link: <https://catalogocloud.acn.gov.it/show/all?searchType=SaaS>

Tale requisito dovrà necessariamente risultare soddisfatto al rilascio e passaggio in produzione del servizio, a pena di risoluzione del contratto.

3. Trattamento dei dati personali

Per tutti i trattamenti di dati personali effettuati nell'ambito dei servizi erogati dal Fornitore al Committente, dovrà essere garantito il rispetto delle vigenti norme, comunitarie e nazionali, in relazione al trattamento di dati personali (Regolamento EU n. 679/2016 - GDPR - General Data Protection Regulation). La conformità dovrà essere garantita sia nella fase di realizzazione ed avvio dei servizi che nell'esercizio a regime nonché a fronte di eventuali variazioni della normativa di riferimento. Tutti gli strumenti utilizzati per le varie funzioni (ad esempio per la reportistica) devono essere conformi al GDPR (ad esempio Google Analytics non è ammesso in quanto deprecato).

Il Fornitore è autorizzato ad effettuare esclusivamente i trattamenti di dati concordati con il Committente e strettamente necessari per l'erogazione dei servizi contrattualmente previsti. Eventuali violazioni saranno opportunamente sanzionate.

Entro l'avvio del servizio il Committente provvederà a nominare con specifico atto il Fornitore quale Responsabile del Trattamento dei dati personali ai sensi del GDPR sulla base dei trattamenti previsti dai requisiti funzionali di cui all'Allegato A2.

4. Misure Minime di Sicurezza ICT

I servizi applicativi dovranno, in tutte le loro componenti, garantire il rispetto di

“Misure minime di sicurezza ICT per le Pubbliche Amministrazioni” di cui alla Circolare AgID 18 aprile 2017, n. 2/2017 <http://www.gazzettaufficiale.it/eli/id/2017/05/05/17A03060/sg>.

- misure di sicurezza ICT previste dall'Allegato A delle “Linee guida AgID - Sicurezza nel Procurement ICT”, di cui alla Determinazione AGID n. 220/2020 del 17 maggio 2020 - Adozione delle Linee Guida – La sicurezza nel procurement ICT. In base alla tipologia della fornitura, come specificato al punto 2.3.15, TABELLA 6 “MATRICE AZIONI TIPOLOGIA-FORNITURA” si determinano i controlli applicabili. https://trasparenza.agid.gov.it/archivio28_provvedimenti-amministrativi_o_122261_725_1.html
- Inoltre, il fornitore dovrà assicurare il rispetto di tutte le misure di sicurezza indicate dall'Agenzia per l'Italia Digitale in vigore al momento della stipula del contratto, nonché di quelle che dovessero essere emanate nel corso della fornitura, con particolare riferimento a:
- Transport Layer Security (TLS) e Cipher Suite, di cui alla Determinazione AGID n. 471 del 5 novembre 2020 - Adozione delle Raccomandazioni AgID in merito allo standard Transport Layer Security (TLS) <https://www.agid.gov.it/it/sicurezza/tls-e-cipher-suite>
- Linee guida per lo sviluppo del software sicuro: <https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro>

Il rispetto di tale requisito dovrà essere garantito sia nella fase di realizzazione ed avvio dei servizi che nell'esercizio a regime nonché a fronte di eventuali variazioni del contesto tecnologico di riferimento.

5. Dislocazione dei datacenter

Il datacenter del Fornitore utilizzati per le seguenti funzioni:

- l'erogazione dei servizi contrattualmente previsti
- lo storage dei dati raccolti e trattati nell'ambito dell'erogazione dei servizi
- i servizi di backup e disaster recovery

dovranno essere dislocati esclusivamente nel territorio dell'Unione Europea.

Qualora i datacenter non siano in Unione Europea è preferibile siano in un paese che abbia un giudizio di adeguatezza da parte della Commissione Europea, oppure che venga fatta una valutazione di impatto del trasferimento dei dati per identificare ulteriori attività a tutela della sicurezza.

L'Appaltatore è tenuto a specificare quali provider intende utilizzare e è tenuto a informare il Committente in caso di variazione.

6. Business continuity e disaster recovery

I servizi applicativi oggetto del contratto dovranno di norma essere tutti attivi ed utilizzabili 24h/giorno e 7 giorni su 7, festivi compresi.

La % di uptime dei servizi applicativi, calcolata su base annua e su tutti e soli i servizi rilasciati in produzione, utilizzando una sonda concordata tra le parti, non dovrà essere inferiore al 99,50%; eventuali violazioni di tale SLA comporteranno l'applicazione di penali, come descritto all'Art. 10 del Capitolato.

Ai fini della determinazione della % di uptime dei servizi applicativi, nel calcolo si terrà conto delle seguenti casistiche:

- Interruzione per interventi di manutenzione programmata, purché effettuati nel rispetto di quanto di sotto specificato;
- Indisponibilità del servizio attribuibile a cause fuori dal ragionevole controllo del Fornitore, inclusi eventi di forza maggiore

Gli interventi di manutenzione programmata dovranno:

- Essere notificati al Politecnico con anticipo di almeno 7 gg
- Avere una durata, per singolo intervento, non superiore alle 8h
- Avere una durata, cumulata sul mese, non superiore alle 16h
- Avere una durata, cumulata sull'anno, non superiore alle 48h

Interventi di manutenzione programmata che violino almeno una delle soglie sopra riportate verranno ricompresi tra le indisponibilità nel computo della % di uptime dei servizi.

A fronte di eventuali guasti che dovessero compromettere la continuità dei servizi applicativi, il Fornitore dovrà garantire il loro ripristino nel rispetto dei seguenti SLA:

- RTO (Recovery Time Objective) dei servizi applicativi = 8h
- RPO (Recovery Point Objective) dei servizi applicativi = 4h lavorative

Con cadenza semestrale, entro 10 gg lavorativi dalla fine del semestre, il Fornitore dovrà produrre un resoconto dei tempi di indisponibilità dei servizi calcolato sulla base della sonda applicativa concordata. Tale resoconto sarà oggetto di validazione da parte del Committente sulla base delle evidenze in proprio possesso e costituirà il riferimento per la determinazione di eventuali penali secondo le modalità descritte all' Art. 10 del Capitolato.

7. Log degli accessi

Il Fornitore dovrà conservare, per almeno 12 mesi ed in modalità conforme a quanto previsto dalla normativa vigente, i log di accesso ai servizi erogati.

Il livello di dettaglio degli eventi registrati nei log verrà concordato con il Committente.

8. Ambiente di test

Il Fornitore dovrà rendere disponibile al Committente accanto all'ambiente di esercizio un ambiente di test con caratteristiche analoghe all'ambiente di esercizio, compreso il collegamento con la Knowledge Base, per consentire ad operatori autorizzati di effettuare prove e simulazioni.

L'ambiente di test dovrà essere disponibile a partire dall'inizio della fase di migrazione e dovrà rimanere attivo ed utilizzabile per tutta la durata del contratto. L'ambiente di test verrà utilizzato per la verifica preventiva rispetto al rilascio in produzione degli aggiornamenti e delle nuove funzionalità rilasciate nel corso dell'esecuzione del contratto.

L'inserimento iniziale dei dati e la sincronizzazione tra i due ambienti sono interamente a carico dell'Appaltatore per l'intera durata contrattuale. Il Committente potrà chiedere una sincronizzazione periodica dell'ambiente di test o potrà fare specifiche richieste di sincronizzazione in occasione di particolari esigenze.

9. Base di dati

Il Fornitore dovrà garantire in qualsiasi momento la possibilità di fornire un'estrazione completa dei dati gestiti dal sistema.

10. Autenticazione ed autorizzazione degli utenti e degli operatori per l'accesso ai servizi

Le funzionalità di autenticazione degli utenti e di autorizzazione di base per l'accesso ai servizi applicativi del Fornitore verranno espletate esclusivamente da servizi resi disponibili dal Politecnico di Milano.

L'accesso ai servizi applicativi del Fornitore da parte degli utenti, qualunque sia la loro categoria di appartenenza, sia lato front-office per l'utente finale che lato back-office per gli operatori, dovrà quindi essere effettuata esclusivamente tramite servizi di autenticazione erogati dal Committente. Nello specifico il sistema del Fornitore dovrà essere compatibile con SAML 2.0 e supportare l'interazione del proprio Service Provider Shibboleth con l'IdP Shibboleth dell'Ateneo. Dovranno essere supportate le funzionalità di Single-Sign-On e single logout.

Non sarà consentita al Fornitore l'assegnazione agli utenti di altre credenziali per l'accesso ai propri servizi, né, in alcuna forma, l'acquisizione e/o la memorizzazione delle credenziali di autenticazione rilasciate dal Politecnico di Milano.

L'integrazione sarà realizzata a carico dell'Appaltatore.

Il Sistema deve prevedere la gestione di una anagrafica degli operatori del back office, a ciascuno dei quali deve essere associato uno specifico profilo che ne definisca il livello di abilitazione:

- gestione delle configurazioni di sistema
- gestione completa o parziale delle varie funzionalità del sistema

Tali abilitazioni devono essere modificabili in qualsiasi momento a cura dell'amministratore di sistema locale, che dovrà essere in grado di eseguire autonomamente, senza necessità di intervento dell'Appaltatore, configurazioni e operazioni funzionali all'erogazione ordinaria dei servizi.

11. Integrazione con altri sistemi

Oltre alle integrazioni e ai servizi web già indicati in altre parti dei documenti di gara il sistema dovrà essere aperto a possibili estensioni e integrazioni con sistemi e servizi esterni tramite api aperte e web services.

Il fornitore indichi gli ambiti per cui sono già disponibili servizi di integrazione e dettagli il tipo di interfaccia utilizzato per permettere di valutarne l'utilità in vista di eventuali future estensioni e il livello di apertura del sistema.

12. Dominio dei server e indirizzi mail utilizzati per le comunicazioni agli utenti

Le parti pubbliche dei servizi erogati (interfaccia utente unificata, A-Z list, link resolver) dovranno preferenzialmente essere registrati nel dominio polimi.it. Se non fosse possibile dovranno comunque essere riconoscibili come polimi.

Gli indirizzi mail utilizzati per le comunicazioni inviate agli utenti dovranno essere obbligatoriamente inviate dal dominio polimi.it.

13. Migrazione storico dati pregressi

Il Fornitore dovrà farsi carico di analizzare la situazione esistente e di provvedere alla migrazione dei dati già presenti nei sistemi in uso presso l'Ateneo (Primo, SFX, Metalib). La tempistica richiesta per la realizzazione di questa attività dovrà essere specificata nel Piano di migrazione e attivazione del servizio richiesto all'Art. 6 del Capitolato.

14. Transitorio di passaggio ai nuovi servizi

L'eventuale disservizio in produzione richiesto per il passaggio da Primo, SFX, Metalib non dovrà superare i 3 giorni lavorativi.

15. Formazione ed affiancamento

Il Fornitore si obbliga - a propria cura e spese - ad erogare attività di formazione tecnica rivolta agli amministratori locali e al personale delle biblioteche. La formazione dovrà venire effettuata durante la fase di

migrazione, dovrà essere articolata in un congruo numero di ore e dovrà avvenire secondo un calendario e con le modalità descritte nella Relazione Tecnica e dovrà essere concordata nel dettaglio in sede di esecuzione con il Committente. La formazione dovrà essere effettuata nel rispetto del piano delle attività previsto nel Capitolato all'art. 6, nei tempi e con le modalità di dettaglio che verranno concordate con il Committente.

La formazione dovrà essere obbligatoriamente erogata in lingua italiana e dovrà poter contare su materiale didattico in italiano e avvalersi dell'utilizzo dell'ambiente di test. Al termine dell'attività di formazione tecnica, dovrà essere rilasciata, a ciascuna unità di personale universitario, idoneo attestato di partecipazione al corso. Dovranno inoltre essere garantite almeno 30h complessive di formazione specifica destinata agli amministratori locali del sistema e agli operatori di back-office delle biblioteche dell'Ateneo. L'attività di formazione dovrà comprendere fasi interattive da erogarsi presso la sede dell'Ateneo o in modalità remota. Dovrà inoltre essere previsto un congruo numero di ore di affiancamento nel transitorio di avvio dei servizi.

16. Documentazione

Il Fornitore dovrà garantire la disponibilità online di adeguata documentazione tecnica e manualistica utente, relativa a tutte le funzioni e moduli applicativi oggetto della fornitura. La documentazione dovrà essere tempestivamente aggiornata con release note in concomitanza di nuovi rilasci.

17. – Servizi di assistenza e manutenzione

Per la gestione delle richieste di assistenza e manutenzione (correttiva, adeguativa, ordinaria, normativa) dovrà essere utilizzato un sistema di trouble ticketing che consenta al Fornitore di registrare l'avanzamento e la chiusura del ticket, e al Committente di verificare lo stato di avanzamento dei ticket aperti e di accedere ai ticket chiusi, anche tramite ricerca di parole chiave nel testo. I ticket dovranno essere gestiti in lingua italiana o eventualmente in inglese.

Si considera preferibile il sistema di trouble ticketing adottato dal Politecnico di Milano (OTRS-OTOB), tuttavia potrà essere accettato anche un sistema di trouble ticketing proposto dal Fornitore, purché sia coerente con i requisiti sopra esposti. In tal caso Il Fornitore dovrà descrivere nella Relazione Tecnica le caratteristiche e le modalità del suo sistema di assistenza per consentirne la valutazione.

Tale sistema costituirà il riferimento per la valutazione degli indicatori dei servizi di assistenza e manutenzione ai fini dell'applicazione di eventuali penali, come descritto all'Art. 10 del Capitolato.

All'interno del sistema di trouble ticketing dovranno essere anche segnalati tempestivamente eventuali incidenti di sicurezza informatica.

a. Manutenzione correttiva

Per "manutenzione correttiva" si intende la diagnosi e la rimozione delle cause e degli effetti dei malfunzionamenti delle procedure, dei programmi e di tutti i componenti del servizio. L'attività di manutenzione correttiva dovrà essere erogata relativamente al software in esercizio, ivi comprese le componenti software che il Fornitore nel corso del periodo contrattuale avrà modificato o realizzato ex-novo nell'ambito della manutenzione normativa, adeguativa ed evolutiva.

Tale attività è innescata da impedimenti all'esecuzione dell'applicazione e/o delle funzioni o da differenze riscontrate fra l'effettivo funzionamento del software applicativo e quello atteso, previsto dalla relativa documentazione o comunque determinato dalla prassi dell'utente.

Il servizio di manutenzione correttiva è pertanto teso alla risoluzione dei difetti presenti nell'applicazione attraverso la diagnosi e la rimozione delle cause e degli effetti, sia sulle interfacce utente che sulle basi di dati, dei malfunzionamenti delle funzionalità e del programma per ripristinarne la piena operatività.

La manutenzione correttiva segue una modalità di erogazione di tipo continuativo ed è, in linea di massima, non pianificabile essendo orientata alla rimozione dei difetti causati dal software stesso.

Gli interventi di manutenzione correttiva dei servizi potranno essere innescati da segnalazioni degli amministratori locali del sistema inserite tramite il sistema di trouble ticketing.. Tali segnalazioni saranno di tipo “malfunzionamento” e verranno così classificate in base alla priorità:

- priorità 0: l'intero sistema è indisponibile agli utenti e l'operatività è completamente bloccata
- priorità 1: una funzionalità critica del sistema (ovvero con scadenza immediata e non surrogabile con altre funzionalità o workaround) risulta indisponibile agli utenti (o presenta gravi malfunzionamenti) e la corrispondente operatività è bloccata;
- priorità 2: una funzionalità non critica del sistema (ovvero priva di scadenza immediata o surrogabile con altre funzionalità o workaround) è indisponibile agli utenti o presenta gravi malfunzionamenti;
- priorità 3: una funzionalità non critica del sistema (ovvero priva di scadenza immediata o surrogabile con altre funzionalità o workaround) presenta malfunzionamenti che non impediscono l'operatività;

Per i servizi di assistenza e manutenzione l'Appaltatore dovrà garantire i seguenti SLA:

Tempo di presa in carico delle segnalazioni di tipo “malfunzionamento” con priorità 0	1h lavorativi dall'inserimento o dalla segnalazione telefonica
Tempo di presa in carico delle segnalazioni di tipo “malfunzionamento” con priorità 1	2h lavorativa dall'inserimento o dalla segnalazione telefonica
Tempo di presa in carico delle segnalazioni di tipo “malfunzionamento” con priorità 2	1 gg lavorativo dall'inserimento
Tempo di presa in carico di altre segnalazioni e richieste	2 gg lavorativi dall'inserimento
Tempo di ripristino del pieno servizio a fronte di malfunzionamenti di priorità 1	8h lavorative dalla presa in carico
Tempo di ripristino del pieno servizio a fronte di malfunzionamenti di priorità 2	24h lavorative dalla presa in carico
Tempo di ripristino del pieno servizio a fronte di malfunzionamenti di priorità 3	48h lavorative dalla presa in carico

Dovranno inoltre essere rese disponibili e comunicate all'avvio dei servizi:

- una linea telefonica attiva in orario d'ufficio (lunedì-venerdì ore 8.30-12.30 – 13.30-17.30) utilizzabile per:
 - segnalazioni di tipo “malfunzionamento” ad elevata priorità (0 o 1)
 - indisponibilità del sistema di trouble-ticketing
 - approfondimenti in relazione a richieste di manutenzione evolutiva
- un indirizzo mail funzionale al quale inviare le richieste e le segnalazioni in caso di indisponibilità del sistema di trouble-ticketing

Con cadenza semestrale l'Appaltatore dovrà produrre un resoconto degli indicatori qualitativi del servizio di assistenza e manutenzione sopra descritti. Tale resoconto sarà oggetto di validazione da parte del Committente sulla base delle evidenze in proprio possesso e costituirà il riferimento per la determinazione di eventuali penali secondo le modalità descritte all' Art. 10 del Capitolato.

b. Manutenzione adeguativa

L'Appaltatore dovrà garantire l'effettuazione di tutti gli interventi di manutenzione adeguativa volti ad assicurare la costante aderenza delle procedure, delle funzioni e delle componenti del servizio all'evoluzione dell'ambiente tecnologico del sistema informativo, come ad esempio adeguamenti necessari per l'aggiornamento dell'infrastruttura tecnologica, per l'aggiornamento di versioni del software di base necessari per garantire la sicurezza dei dati e del servizio e l'applicazione di corrispondenti aggiornamenti di sicurezza sulle varie componenti del servizio non appena queste vengono rilasciate dai produttori.

L'attività di manutenzione adeguativa dovrà essere erogata relativamente al servizio in esercizio, ivi comprese le funzionalità che l'Appaltatore nel corso del periodo contrattuale avrà modificato o realizzato ex-novo.

c. Manutenzione ordinaria

Il servizio di manutenzione ordinaria prevede il rilascio periodico di nuove release, contenenti migliorie e implementazioni rese disponibili per la comunità degli utilizzatori dell'applicativo, e della relativa documentazione.

d. Manutenzione per adeguamenti normativi

L'Appaltatore dovrà implementare, in accordo con il Committente, tutti gli adeguamenti normativi delle applicazioni che si rendessero necessari per gli ambiti ricompresi nei servizi oggetto della fornitura per effetto di nuove disposizioni di legge e/o di regolamenti governativi per l'applicazione delle leggi stesse.

A titolo esemplificativo, ma non esaustivo, sono da intendere come adeguamento normativo le modifiche da apportare alle applicazioni in seguito a variazioni di regolamenti e norme in materia di sicurezza e protezione dati.

In linea di massima, l'adeguamento normativo legato a mutamenti normativi di carattere nazionale ed europeo che hanno ricadute sul servizio sia sotto il profilo tecnico che di contesto di applicazione, sono dovute senza che sia effettuata esplicita richiesta da parte dell'Università.

Le attività di manutenzione normativa possono anche essere effettuate sulla base di richieste esplicite da parte dell'università attraverso il portale di trouble-ticketing.

Tutte le attività descritte ai punti a, b, c, d (manutenzione correttiva, adeguativa, ordinaria e normativa) sono da considerarsi già incluse nel costo del servizio e non comporteranno alcun onere aggiuntivo per il Politecnico di Milano.

18. Supporto al termine del contratto

L'Appaltatore dovrà garantire, senza ulteriori oneri per l'Università, supporto e collaborazione per ottenere la corretta ed efficace migrazione dei dati verso un nuovo Fornitore di servizio alla cessazione del contratto.

19. Supporto in caso di cessazione del contratto

L'Appaltatore si impegna, senza costi aggiuntivi, in caso di interruzione del rapporto a fornire i dati in modo fruibile, in formato concordato e comunque utilizzabile dall'Amministrazione, corredati di adeguata documentazione tecnica relativa alla struttura dati.

L'eventuale inottemperanza a questo punto essenziale verrà considerata interruzione di pubblico servizio. Dovrà inoltre fornire il supporto per la migrazione dei dati di proprietà dell'Amministrazione dal proprio sistema a quello di un eventuale nuovo Fornitore subentrante.

L'Appaltatore è inoltre tenuto, salvo nei casi previsti dalla legge, a cancellare dalla piattaforma tutti i dati di proprietà del Politecnico di Milano.

20. Attività di Audit

Al fine di garantire un adeguato livello di Compliance normativa e regolamentare, il Politecnico di Milano si riserva di attuare periodiche attività di internal audit in merito ai processi e ai sistemi di gestione integrati

operanti all'interno dell'Ateneo con l'obiettivo di valutare l'adeguatezza dei controlli interni dell'Organizzazione - finalizzati alla corretta gestione dei rischi - e lo svolgimento di attività di monitoraggio periodico in merito agli stessi nonché la diffusione della cultura e delle relative pratiche di miglioramento continuo.

Le attività di internal audit, svolte nel rispetto dei principi di imparzialità e indipendenza, possono impattare anche fornitori e terze parti a qualsiasi titolo coinvolti nell'erogazione dei servizi oggetto di questo contratto.

Sempre al fine di garantire un adeguato livello di Compliance normativa e regolamentare, il Fornitore – in qualità di Responsabile del trattamento – si impegna a svolgere attività periodiche di internal audit in merito ai processi e ai sistemi informatici che trattano dati personali di cui il Politecnico di Milano è titolare, fornendone puntuale riscontro al Politecnico stesso. Rispetto alle non conformità e ai rischi emersi nel corso delle analisi di audit interno, il Fornitore si impegna inoltre ad attivare opportuni e mirati piani di rientro nonché a comunicare al Politecnico di Milano la data prevista per implementare la relativa azione di rientro.

Il Fornitore si impegna a cooperare, mettendo a disposizione tutta la documentazione e le informazioni che saranno richieste dal Politecnico di Milano il quale, d'altro canto, si impegna a svolgere esclusivamente a proprie spese le attività di audit che riterrà necessarie nei riguardi del Fornitore.

Tutte le attività saranno svolte al fine di valutare la conformità del trattamento dei dati posto in essere rispetto alla vigente normativa di settore nonché rispetto alle istruzioni impartite dal titolare del trattamento e, naturalmente, alle indicazioni fornite dal presente documento; le attività di audit saranno inoltre condotte al fine di valutare la corrispondenza fra le misure tecnico-organizzative effettivamente implementate e quelle dichiarate all'interno dell'offerta tecnica presentata per l'adesione al bando di gara.

Il Politecnico di Milano si impegna a garantire un congruo preavviso al Fornitore (10 giorni) al fine di consentire - da ambo le parti - la migliore organizzazione possibile delle rispettive attività, evitando in tal modo di venire a gravare eccessivamente sulla programmazione delle ordinarie attività ed evitando rallentamenti nell'esecuzione dei progetti; una puntuale e preventiva organizzazione delle attività di audit garantirà inoltre al Fornitore lo svolgimento delle stesse nel corso dell'ordinario orario lavorativo.

Contestualmente alla comunicazione relativa all'avvio delle attività di audit, il Politecnico di Milano si impegna a rendere noti i parametri di valutazione, le modalità e i servizi oggetto di analisi