Allegato 2 - Requisiti generali inderogabili dei servizi

1. Titolarità del software e dei dati

Il Committente è sempre titolare:

- del software sviluppato o messo a disposizione dal Fornitore, inclusi i template grafici ed i moduli personalizzati, oltre ai relativi codici sorgente ed alla documentazione, fatto salvo l'utilizzo di componenti software già esistenti (es: librerie e framework open source o di terzi) per le quali è necessario acquisire la licenza d'uso (che deve essere compatibile con le finalità di riuso).
- di tutti i dati e di tutti i contenuti dei servizi sviluppati, inclusi a titolo esemplificativo e non esaustivo: testi, video, immagini, file audio, etc.

2. Misure Minime di Sicurezza ICT e normativa di riferimento

I servizi erogati dovranno, in tutte le loro componenti, garantire il rispetto dei seguenti atti normativi e di indirizzo:

- Decreto legislativo 7 marzo 2005, n. 82 e ss.mm.ii., recante "Codice dell'Amministrazione Digitale";
- Direttiva 27 luglio 2005 della Presidenza del Consiglio dei ministri – Dipartimento per l'Innovazione e le Tecnologie recante "Qualità dei servizi online e misurazione della soddisfazione degli utenti";
- Provvedimento generale 27 novembre 2008 (e ss.mm.ii.) dell'Autorità garante per la protezione dei dati personali, recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";
- Decreto legislativo 25 maggio 2016, n. 97 "Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche";
- Regolamento generale sulla protezione dei dati" UE n. 679/16;
- D.Lgs 10 agosto 2018, n. 101 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche;
- Provvedimento 10 giugno 2021, n° 231 dell'Autorità garante per la protezione dei dati personali, recante "Linee guida cookie e altri strumenti di tracciamento";
- Normativa di riferimento in materia di accessibilità digitale:
  https://www.agid.gov.it/it/design-servizi/accessibilita/normativa
  e rispettive linee guida AGID;
  https://www.agid.gov.it/it/design-servizi/accessibilita/linee-guida-accessibilita-pa;
- Linee guida di design per i siti internet e i servizi digitali della PA https://docs.italia.it/italia/design/lg-design-servizi-web/it/versione-corrente/index.html;
- "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 .
- Requisiti di sicurezza ICT individuati come rilevanti per la fornitura sulla base della Tabella 6 "Matrice azioni tipologia-fornitura" del punto 2.3.15 delle "Linee guida AgiD - Sicurezza nel Procurement ICT"

https://trasparenza.agid.gov.it/archivio28_provvedimenti-amministrativi_0_122261_725_1.html (Determinazione AGID n. 220/2020 del 17/05/2020) e descritti nell'Appendice A di tale documento;

- 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 AgID per lo sviluppo del software sicuro: https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro;
- Poichè l'Ateneo rientra nell'ambito di applicazione della direttiva NIS2 (DLGS n. 134 del 04/09/2024) come soggetto importante, nei contratti attuativi dell'Accordo Quadro potrà essere richiesto che siano soddisfatti i requisiti pertinenti la richiesta di servizio.

Il rispetto di tutti i requisiti sopra esposti dovrà essere garantito sia nella fase di realizzazione ed avvio dei servizi che nell'erogazione a regime per tutta la durata dei contratti attuativi, anche a fronte di eventuali variazioni del contesto tecnologico di riferimento o normativo di competenza (es. aggiornamento delle "Misure minime di sicurezza ICT per le Pubbliche Amministrazioni" da parte di AgID). I servizi richiesti dovranno in ogni caso essere erogati nel rispetto di ogni altro requisito in materia imposto dalla normativa vigente o sopravvenuta.

3. Requisiti generali dei servizi sviluppati

Il Fornitore dovrà certificare e garantire per i servizi sviluppati la compatibilità con i browser più diffusi (Chrome, Safari, FireFox, Edge) e con le loro successive evoluzioni.
Le interfacce Web dovranno:

- 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 predisposta per il multilinguismo e localizzata in italiano e inglese.
- essere conforme ai requisiti di accessibilità in ottemperanza alla normativa vigente https://www.agid.gov.it/it/design-servizi/accessibilita/normativa e alle linee guida AGID https://www.agid.gov.it/it/design-servizi/accessibilita/linee-guida-accessibilita-pa

4. Modalità di erogazione dei servizi sviluppati

I siti web potranno essere sviluppati in base alle richieste di servizio del Committente:

- sulle piattaforme di hosting rese disponibili dall'Area Servizi ICT del Politecnico di Milano, che ha in carico la gestione sistemistica di tali piattaforme, come specificato nel documento https://www.ict.polimi.it/hosting/hosting-siti-internet-e-applicazioni-web/;
- su piattaforme cloud gestite dal Fornitore.

Qualora siano richiesti servizi cloud:

- tali servizi dovranno essere erogati in modalità SaaS tramite piattaforme qualificate dall'Agenzia per la Cybersicurezza Nazionale www.acn.gov.it e pubblicate sul "Catalogo dei servizi Cloud per la PA qualificati" dell'ACN Cloud Marketplace.
- il datacenter dove saranno collocati:

- i server utilizzati per l'erogazione dei servizi contrattualmente previsti;
- i dati raccolti e trattati nell'ambito dell'erogazione dei servizi;
- i siti di backup e disaster recovery;

dovranno essere dislocati esclusivamente nel territorio dell'Unione Europea.

5. 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, sia nella fase di realizzazione ed avvio dei servizi che nell'esercizio a regime, nonché a fronte di eventuali variazioni della normativa di riferimento.

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.

Le strutture del Politecnico di Milano richiedenti i servizi oggetto dell'accordo quadro, nell'ambito dei rispettivi contratti attuativi nomineranno autonomamente il Fornitore quale Responsabile del Trattamento dei dati personali, se necessario per lo svolgimento delle attività oggetto delle richieste di servizio sottoposte dalle strutture stesse.

6. Business continuity e disaster recovery per servizi SaaS

I siti web erogati in modalità SaaS (rif. paragrafo 4 – Modalità di erogazione dei servizi sviluppati) dovranno di norma essere tutti attivi ed utilizzabili 24h/giorno e 7 giorni su 7, festivi compresi.

La % di uptime dei siti web, calcolata su base semestrale e su tutti e soli i servizi rilasciati in produzione, non dovrà essere inferiore al 99,70%.

Ai fini della determinazione della % di uptime dei siti web, 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
- indisponibilità del servizio attribuibile a interventi di manutenzione sull'infrastruttura fornita da ASICT

Gli interventi di manutenzione programmata dovranno:

- essere notificati al Politecnico con anticipo di almeno 10gg lavorativi
- avere una durata, per singolo intervento, non superiore alle 4h lavorative
- avere una durata, cumulata sul mese, non superiore alle 8h lavorative
- avere una durata, cumulata sul semestre, non superiore alle 24h lavorative

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 malfunzionamenti che dovessero compromettere la continuità dei servizi, il Fornitore dovrà garantire il loro ripristino nel rispetto dei seguenti SLA:

- RTO (Recovery Time Objective) dei siti web = 8h solari

- RPO (Recovery Point Objective) dei siti web = 4h solari

Il Fornitore potrà proporre nella propria Offerta Tecnica condizioni migliorative rispetto a:

- Disponibilità dei siti web (% Uptime)
- RTO (Recovery Time Objective) dei siti web
- RPO (Recovery Point Objective) dei siti web

Di tali condizioni migliorative si terrà conto nella valutazione delle offerte tecniche. Le eventuali condizioni migliorative offerte costituiranno le nuove soglie minime, superate le quali ricorreranno le condizioni per l'applicazione delle rispettive penali.

Eventuali violazioni degli SLA sopra descritti comporteranno l'applicazione di penali per il mancato rispetto dei livelli di servizio contrattualmente definiti.

Con cadenza semestrale, entro 10 gg lavorativi dalla fine del semestre, il Fornitore dovrà produrre un resoconto dei tempi di indisponibilità dei servizi. 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.

7. Vulnerability Assessment per servizi SaaS

Per i siti web erogati in modalità SaaS (rif. paragrafo 4 – Modalità di erogazione dei servizi sviluppati) il Fornitore dovrà eseguire Vulnerability Assessment (VA):

- prima del rilascio in produzione del sito web;
- con cadenza almeno semestrale dal rilascio in produzione del sito web;
- conformi alla metodologia OWASP WEB Security Testing Guide https://owasp.org/www-project-web-security-testing-guide/#div-faq

Il Fornitore si impegna a:

- inviare al Committente, entro 30 giorni dall'esecuzione di ogni VA, il report dei risultati e il rispettivo piano di remediation che indirizzi puntualmente le eventuali vulnerabilità emerse;
- risolvere le eventuali vulnerabilità di livello critico entro 3 mesi dalla rilevazione.

Per i siti web erogati in modalità SaaS da terzi per i quali venga richiesta da Politecnico di Milano l'esecuzione del Vulnerability Assessment (VA), il Fornitore dovrà:

- svolgere con la frequenza richiesta l'attività in modalità conforme alla metodologia OWASP WEB Security Testing Guide https://owasp.org/www-project-web-security-testing-guide/#div-faq
- inviare al Committente, entro 30 giorni dall'esecuzione di ogni VA, il report dei risultati e il rispettivo piano di remediation che indirizzi puntualmente le eventuali vulnerabilità emerse;
- risolvere le eventuali vulnerabilità di livello critico entro 3 mesi dalla rilevazione.

Eventuali violazioni degli SLA sopra descritti comporteranno l'applicazione di penali per il mancato rispetto dei livelli di servizio contrattualmente definiti.

8. Log degli accessi

Il Fornitore dovrà conservare, per 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 dovrà essere concordato con il Committente e comunque dovrà rispettare quanto indicato da AGID alle "Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni" https://www.agid.gov.it/it/infrastrutture/sistema-pubblico-connettivita/il-nuovo-modello-interoperabilita

9. Ambiente di test

Nell'ambito di contratti attuativi relativi a servizi SaaS, il Fornitore dovrà rendere disponibile al Committente, per l'intera durata contrattuale, un completo ambiente di test dei siti web sviluppati.

Tale ambiente verrà utilizzato per la verifica, preventiva rispetto al passaggio in produzione, degli aggiornamenti e delle nuove funzionalità rilasciate nel corso dell'esecuzione del contratto.

10. Base di dati

Nell'ambito di contratti attuativi relativi a servizi SaaS, il Fornitore dovrà garantire, a personale specificatamente incaricato dal Committente, l'accesso in sola lettura all'intero schema del database di test e di produzione. Di tale schema dovrà essere fornita dettagliata documentazione (descrizione tabelle, campi e relazioni) che dovrà essere aggiornata in corrispondenza dei rilasci di nuove versioni. Tale documentazione sarà di supporto sia alla gestione operativa che al passaggio verso un nuovo Fornitore di servizio alla cessazione dei contratti attuativi.

11. Autenticazione ed autorizzazione degli utenti per l'accesso ai servizi

Le funzionalità di autenticazione degli utenti e di autorizzazione di base per l'accesso ai siti web oggetto dei contratti attuativi verranno espletate esclusivamente da servizi resi disponibili dal Politecnico di Milano.

L'accesso autenticato da parte degli utenti ai siti web, qualunque sia la loro categoria di appartenenza, 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.

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

12. Integrazione con altri sistemi

Nel caso siano richieste integrazioni ulteriori rispetto a quanto indicato sopra e al punto precedente dovranno essere concordati e specificati:

- articolazione dettagliata delle strutture dati oggetto di allineamento;
- interfacce e protocolli di interfacciamento tra i sistemi;
- modalità di gestione delle condizioni anomale e degli errori.

Saranno a totale carico del Fornitore tutte le attività necessarie per l'analisi, la progettazione, lo sviluppo, la messa a punto e l'erogazione delle integrazioni, nel pieno rispetto dei requisiti definiti dal Committente.

13. Formazione ed affiancamento

Nell'ambito di ogni contratto attuativo il Fornitore dovrà garantire almeno 16h lavorative di formazione specifica e destinata al personale del Committente per le varie tipologie di gestori e di utilizzatori dei siti web richiesti, che dovrà coprire tutte le funzionalità implementate nei siti stessi.

14. Documentazione

Il Fornitore dovrà garantire la disponibilità online di adeguata documentazione tecnica e manualistica utente, relativa ai servizi erogati nell'ambito dei contratti attuativi, che dovrà essere tempestivamente aggiornata con release note in concomitanza di nuovi rilasci e dello sviluppo di nuove funzionalità.

I siti web dovranno essere predisposti per il multilinguismo e localizzati in italiano e inglese.

Al termine di ogni contratto attuativo, il Fornitore si impegna a rilasciare, senza costi aggiuntivi, la seguente documentazione finale e completa dei servizi erogati:

A. manuale di installazione e/o di configurazione;
B. report degli assessment di sicurezza eseguiti con l'indicazione delle eventuali vulnerabilità riscontrate e delle azioni di risoluzione/mitigazione apportate;

C. "libretto di manutenzione", con l'indicazione delle attività da eseguire per mantenere un adeguato livello di sicurezza dei servizi; in particolare, all'interno del libretto di manutenzione deve essere indicato quanto segue:

- produttore e versione dei prodotti software utilizzati (ad esempio web server, application server, CMS, DBMS), librerie, …;
- indicazioni per il reperimento dei Bollettini di Sicurezza dei singoli produttori dei software utilizzati;
- indicazioni sul processo di installazione degli aggiornamenti sicurezza;
- documento di EoL (documento che contiene indicazione dei prodotti utilizzati e relativo fine vita/rilascio degli aggiornamenti di sicurezza).

Con particolare riferimento alle procedure operative che riguardano la sicurezza, il Politecnico di Milano si impegna a comunicare tempestivamente al fornitore - nonché a tutte le strutture interne a qualsiasi titolo coinvolte - tutti gli aggiornamenti, modifiche e/o integrazioni che intervengano nel corso del rapporto contrattuale; d'altro canto, una volta ricevuta la comunicazione delle nuove procedure di sicurezza in essere, sarà cura del fornitore provvedere ad adeguarsi immediatamente ad esse.

15. Servizi di assistenza e manutenzione

Nell'ambito dei contratti attuativi potranno essere richiesti servizi di assistenza e manutenzione per siti web esistenti o di nuova realizzazione. Tali servizi si applicano:

- all'intero stack del servizio SaaS per i siti web sviluppati su piattaforme cloud gestite dal fornitore;
- ai CMS e relative estensioni, plugin e customizzazioni e al codice sorgente per i siti web ospitati su piattaforme gestite da ASICT.

Per la gestione delle richieste di assistenza e manutenzione (correttiva, normativa, adeguativa ed evolutiva), dovrà essere utilizzato esclusivamente il sistema di trouble ticketing di Ateneo basato su OTOBO, nel quale dovranno essere anche segnalati tempestivamente eventuali incidenti di sicurezza informatica.

Il sistema di trouble ticketing sarà reso disponibile dal Committente e sarà lo strumento tramite il quale gli utenti dell'Ateneo inseriranno le richieste e le segnalazioni ed il Fornitore ne registrerà l'avanzamento e la chiusura. Tale sistema costituirà il riferimento per la valutazione degli indicatori dei servizi di assistenza e manutenzione ai fini dell'applicazione di eventuali penali.

15.1. 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 sito web 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 nel codice sorgente, o nelle specifiche di formato o dei dati 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 utenti dell'Ateneo 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 il Fornitore dovrà garantire i seguenti SLA:

Tempo di presa in carico delle segnalazioni di tipo "malfunzionamento" con priorità 0	30min lavorativi dall'inserimento o dalla segnalazione telefonica
Tempo di presa in carico delle segnalazioni di tipo "malfunzionamento" con priorità 1	1h lavorativa dall'inserimento o dalla segnalazione telefonica
Tempo di presa in carico delle segnalazioni di tipo "malfunzionamento" con priorità 2	4h lavorative dall'inserimento
Tempo di presa in carico delle segnalazioni di tipo "malfunzionamento" con priorità 3	8h lavorative dall'inserimento
Tempo di ripristino del pieno servizio a fronte di "malfunzionamenti" di priorità 0	Si vedano RTO e RPO definiti al paragrafo 6. **Business continuity e disaster recovery**
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, entro 10 gg lavorativi dalla fine del semestre, il Fornitore 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.

15.2. Manutenzione adeguativa

Il Fornitore dovrà inoltre 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 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 il Fornitore nel corso del periodo contrattuale avrà modificato o realizzato ex-novo.

15.3. Adeguamenti normativi

Il Fornitore dovrà implementare, in accordo con il Committente, tutti gli adeguamenti normativi che si rendessero necessari per gli ambiti ricompresi nei servizi oggetto dei contratti attuativi 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 ai siti web in seguito a variazioni di regolamenti e norme in materia di sicurezza e protezione dati.

Le attività di adeguamento normativo sono già incluse nel costo del servizio e non comporteranno alcun onere aggiuntivo per il Politecnico di Milano

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 del Politecnico.

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

I rilasci dei corrispondenti aggiornamenti dovranno essere effettuati, dapprima in ambiente di test e successivamente in produzione, in tempo utile per consentire al Politecnico di Milano il rispetto delle scadenze fissate dalla normativa.

15.4. Manutenzione evolutiva

Per "Manutenzione evolutiva" si intende l'attività di manutenzione volta a migliorare le funzionalità dei siti web per assicurare una sempre crescente aderenza delle procedure alle esigenze di automazione ed integrazione con l'ambiente informativo circostante o che si rendessero necessarie a seguito di variazioni regolamentari proprie dell'Università.

L'attività di manutenzione evolutiva dovrà essere erogata relativamente al software in esercizio, ivi comprese le componenti che il Fornitore avrà modificato o realizzato ex-novo nel corso del periodo contrattuale.

Non sono considerate evolutive eventuali correzioni di bug, in quanto incluse nei servizi di assistenza e di manutenzione correttiva ed adeguativa.

16. Supporto al termine dei contratti attuativi

Il Fornitore dovrà garantire, senza ulteriori oneri per il Politecnico di Milano, supporto e collaborazione per ottenere un corretto ed efficace passaggio di consegne verso un nuovo Fornitore di servizio alla cessazione dei contratti attuativi.

17. Supporto in caso di cessazione dei contratti attuativi

Il Fornitore si impegna, senza costi aggiuntivi, in caso di interruzione di un contratto attuativo, a fornire dati e informazioni in modo fruibile, in formato concordato e comunque utilizzabile dall'Amministrazione, corredati di adeguata documentazione tecnica.

Il Fornitore è tenuto inoltre, in fase di transizione iniziale delle attività, a fornire il supporto utile al successivo fornitore in modo da far sì che esso possa collocarsi al meglio nell'ambito del processo e comprendere sia gli aspetti organizzativi sia gli aspetti tecnologici. Al fine di agevolare la fase di transizione di cui sopra, il Politecnico di Milano prevede l'esecuzione di un processo di handover utile a recepire in modo rapido ed efficace tutti gli elementi utili, basato sui seguenti passaggi relativi al trasferimento di conoscenze dal fornitore uscente al fornitore entrante:

a. Passare le conoscenze in merito al servizio fornito al Politecnico di Milano ed alla sua organizzazione, per consentire al fornitore entrante di identificare tutti gli interlocutori ed attori necessari ad effettuare un governo completo del processo.

b. Passare le conoscenze in merito Linee Guida, Policy e Best Practice in ambito, al fine di consolidare il contesto documentale e le regole di riferimento definite da osservare durante l'esecuzione delle attività.

c. Passare le conoscenze in merito agli strumenti a supporto delle attività, per permettere al nuovo fornitore di avere piena padronanza degli strumenti e delle logiche di utilizzo nell'ambito del processo.

L'eventuale inottemperanza a quanto sopra descritto verrà considerata interruzione di pubblico servizio. Nel caso di servizi erogati in modalità SaaS il Fornitore dovrà inoltre garantire il supporto per la migrazione dei servizi e dei dati di proprietà del Committente dal proprio sistema a quello di un eventuale nuovo Fornitore subentrante.

18. 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 dell'Ateneo; tali attività, svolte nel rispetto dei principi di imparzialità e indipendenza, potranno impattare anche fornitori e terze parti a qualsiasi titolo coinvolti nell'erogazione dei servizi oggetto di questo contratto.

Il Fornitore si impegna a cooperare, mettendo a disposizione tutta la documentazione e le informazioni che saranno richieste dal Politecnico di Milano a supporto delle attività di audit che riterrà necessarie nei riguardi del Fornitore. Tali attività saranno svolte al fine di valutare la conformità del trattamento dei dati posto in essere rispetto:

- alla vigente normativa di settore
- alle istruzioni impartite dal titolare del trattamento
- 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 previste nell'ambito dei contratti attuativi.

Il Politecnico di Milano si impegna a garantire per le attività di audit un congruo preavviso al Fornitore (almeno 5 giorni lavorativi) al fine di consentire - da ambo le parti - la migliore organizzazione possibile delle rispettive attività, evitando in tal modo di gravare eccessivamente sulla programmazione delle ordinarie attività ed evitando rallentamenti nell'esecuzione dei progetti.

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.

Sempre al fine di garantire un adeguato livello di compliance normativa e regolamentare, il Fornitore – nell'ambito dei contratti attuativi rispetto ai quali è nominato Responsabile del trattamento dei dati personali – dovrà a sua volta 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 eventuali non conformità e ai rischi emersi nel corso delle attività di audit, il Fornitore dovrà definire specifici piani di rientro che dovranno essere approvati dal Politecnico di Milano ed attuati nel pieno rispetto della tempistica concordata.

Eventuali non conformità particolarmente critiche potranno comportare, ad insindacabile giudizio del Politecnico di Milano, la temporanea sospensione dell'erogazione dei servizi oggetto dell'audit. Tale sospensione verrà computata ai fini della determinazione della % di uptime dei servizi.

19. Riservatezza

Il Fornitore si impegna a conservare il più rigoroso riserbo in ordine a tutta la documentazione fornita dal Politecnico di Milano.

Il Fornitore si impegna altresì a non divulgare a terzi e a non utilizzare per fini estranei all'adempimento dell'accordo stesso procedure, notizie, dati, atti, informazioni o quant'altro relativo al Politecnico di Milano e al suo know-how; a tal fine, si impegna a presentare una certificazione di avvenuta distruzione dei dati oggetto del trattamento e contenente una puntuale indicazione delle modalità utilizzate.

Il Fornitore si impegna altresì a restituire al Politecnico di Milano, entro 10 giorni dall'ultimazione delle attività commissionate, tutti gli atti ed i documenti alla stessa forniti dal Committente ed a distruggere, ovvero rendere altrimenti inutilizzabili, ogni altro atto sia in formato cartaceo che digitale.

Eventuali violazioni commesse dal Fornitore sulle disposizioni di cui al presente paragrafo saranno sanzionate ai sensi della normativa vigente in materia.