MISURE DI SICUREZZA ICT

SERVIZIO DI GESTIONE DELLE PROVE CONCORSUALI IN FORMA DIGITALE

Il Fornitore, qualora utilizzi strumenti informatici per la gestione del servizio, si impegna a adottare le seguenti misure di sicurezza ICT riportate nelle tabelle sottostanti.

1.	***DATI GENERALI***
1.1.	**Banche dati e superficie di attacco**
1.1.1.	Anagrafiche dei candidati alle prove concorsuali. Informazioni sulle capacità psico-motorie e cognitive.
1.2.	**Tipologia connessione | interventi remoti**
1.2.1.	Nessuna connessione a Internet durante le prove concorsuali.
1.3.	**Interventi in sede**
1.3.1.	SI
1.4.	**SUB-APPALTO**
1.4.1.	Qualora il Responsabile Esterno debba utilizzare un sub-appalto, lo stesso responsabile oltre a fare la nomina di Sub-Responsabile alla società/ditta che svolge il sub-appalto, deve richiedere la sottoscrizione di queste misure di sicurezza alla stessa società/ditta. Tale nomina di Sub-Responsabile e misure di sicurezza dovranno essere consegnate anche al Comune di Olbia. Il Sub-Responsabile dovrà effettuare, per il personale che intende utilizzare per le attività oggetto del contratto tra il Comune di Olbia e il Responsabile Esterno, la nomina degli autorizzati al trattamento; una copia di tale nomina deve essere consegnata anche al Comune di Olbia. Tutte le nomine sopra riportate devono essere digitali e firmate digitalmente.

2.	***MISURE ADEGUATE INTERNE ALLA RETE DEL TITOLARE***

3.	***MISURE ADEGUATE SU <u>AMBIENTE</u> DEL RESPONSABILE ESTERNO E DI EVENTUALI SUB-RESPONSABILI*** ***Tali misure sono da applicare obbligatoriamente qualora l'attività svolta dal Responsabile Esterno relativamente al contratto in essere, viene effettuata attraverso il proprio Sistema Informatico (PC, Server, etc.).***
3.1.	**INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI**
3.1.1.	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione
3.2.	**PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER**
3.2.1.	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).
3.2.2	Dispositivi come telefoni cellulari, tablet, laptop, dischi esterni, chiavette USB, Schede SD e altri dispositivi elettronici portatili che memorizzano o elaborano dati dell'Ente, **devono essere criptati**.
3.3.	**VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ**
3.3.1.	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.*).
3.3.2.	Possedere un Piano di Disaster Recovery e di backup sia sulla componente elaborativa (*server*) che sui dati.
3.4.	**USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE**
3.4.1.	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.
3.4.2.	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.
3.4.3.	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.

3.4.4.	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.
3.4.5.	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.
3.4.6.	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).
3.4.7.	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.
3.4.8.	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (*password aging*).
3.4.9.	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (*password history*).
3.4.10.	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.
3.4.11.	Tutte le utenze, in particolare quelle amministrative, devono essere nominative e riconducibili ad una sola persona.
3.4.12.	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, devono essere utilizzate solo per le situazioni di emergenza e le relative credenziali devono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.
3.4.13.	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (*e.g. dominio*).
3.4.14.	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.
3.4.15.	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.
3.5.	**DIFESE CONTRO I MALWARE**
3.5.1.	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 devono essere mantenuti aggiornati in modo automatico.
3.5.2.	**Installare su tutti i dispositivi firewall ed IPS personali**. Per i dispositivi all'interno di una rete dati, deve essere implementata la difesa attraverso Firewall e IPS centralizzati.
3.5.3.	**Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (*syslog*) dove sono stabilmente archiviati.**
3.5.4.	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.
3.5.5.	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.
3.5.6.	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.
3.5.7.	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.
3.5.8.	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.
3.5.9.	Disattivare l'apertura automatica dei messaggi di posta elettronica.
3.5.10.	Disattivare l'anteprima automatica dei contenuti dei file.
3.5.11.	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.
3.5.12.	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.
3.5.13.	Filtrare il contenuto del traffico web.
3.5.14.	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).

4.	***MISURE ADEGUATE AL TRATTAMENTO DEL SISTEMA INFORMATIVO DEL TITOLARE***
4.1.	**TRASMISSIONE TELEMATICA DI DOCUMENTAZIONE**
4.1.1.	La trasmissione telematica di un documento digitale a mezzo di PEC, E-Mail, FTPs, HTTPs, Cisco WebEX, MS-Teams, dovrà essere eseguita inviando la copia criptata del documento: la password/chiave per decifrare dovrà essere inviata separatamente con altra comunicazione.
4.1.2.	Qualunque altro mezzo di trasmissione si voglia utilizzare, diverso da quelli indicati al punto 4.1.1., dovrà essere autorizzato dal responsabile ICT dell'Ente.
4.2.	**COPIE DI SICUREZZA (*Backup di banche dati digitali*)**
4.2.1.	Il Fornitore deve garantire che il sistema effettui ***giornalmente*** una copia di sicurezza ***cifrata*** delle informazioni strettamente necessarie per il completo ripristino del sistema. Il Fornitore deve anche prevedere la raccolta e conservazione dei **logs di sistema** (*server, firewall, antivirus, sistemi operativi, database, applicazioni, servizi cloud, ecc.*) al fine di rilevare incidenti di sicurezza e supportare le attività di investigazione. Anche per queste raccolte di logs deve essere previsto un backup giornaliero.
4.2.1.	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. È preferibile l'utilizzo della copia immutabile del backup.
4.2.1.	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.
4.3.	**COPIE DI DATI**
4.3.1.	**È autorizzata** la copia di dati di cui è Titolare il Comune di Olbia presso l'organizzazione del Fornitore, relativamente ai soli dati necessari all'espletamento della fornitura/servizio, per le finalità del contratto in essere.
4.3.2.	**Non sono autorizzati** i trasferimenti su cloud di documenti contenenti dati di utenti del Comune di Olbia o dei dati presenti sui database ai quali il Fornitore ha accesso per la sola manutenzione, a meno che non siano espressamente autorizzati dal Comune di Olbia e che il Cloud provider sia GDPR Compliant (*server all'interno della UE*) e certificato ACN.

4.3.3.	**Al Fornitore e ai sui tecnici autorizzati al trattamento è fatto divieto assoluto di divulgazione di informazioni del sistema informatico utilizzato e soprattutto dei dati di cui è titolare il Comune di Olbia.**
4.3.4.	Alla fine del contratto, si richiede la distruzione (*con metodi sicuri, autorizzati e supervisionati dal Comune di Olbia*) di eventuali dati in possesso del Fornitore che vadano oltre le finalità del contratto in essere con il Comune. **Per quei dati che per norma di legge, o per disposizioni contrattuali, debbano essere conservati per un periodo che va oltre la scadenza del contratto, deve essere garantita la distruzione (*con metodi sicuri, autorizzati e supervisionati dal Comune di Olbia*) alla fine di tale periodo di conservazione.**
4.3.5.	Nel caso di banche dati di tipo analogico, ad esempio registri cartacei, deve essere garantita la custodia delle stesse limitando l'accesso ai soli autorizzati al trattamento. Devono essere anche messi in sicurezza da accessi non autorizzati gli ambienti dove tali banche dati analogiche vengono conservate. **L'uso di banche dati analogiche deve essere limitato il più possibile e l'eventuale necessità come alternativa ad un sistema digitale deve essere, comunque, concertato con il Servizio ICT del Comune di Olbia.**
4.4.	**ALTRE ATTIVITA'**
4.4.1.	Alla chiusura del contratto viene garantito il punto 4.3.4. sulla distruzione di eventuali dati in possesso del Fornitore, contenenti qualsivoglia dato personale di cui il titolare è il Comune di Olbia.
4.4.2.	**Le eventuali interfacce web utilizzate dal Fornitore dovranno essere criptate (certificati SSL).**
4.4.3.	È fatto obbligo al fornitore la dichiarazione di distruzione delle banche dati di cui ai punti 4.3.4., 4.4.1., 4.4.7., 4.4.9. e 4.4.10., sottoscritta digitalmente e inviata alla PEC del protocollo generale dell'Ente: ***protocollo@pec.comuneolbia.it***.
4.4.4.	**Nel caso di servizio che preveda l'utilizzo di Software in modalità SaaS, sia il Software che il DataCenter, messi a disposizione dal Fornitore, devono essere certificati ACN**.
4.4.5.	Le comunicazioni contenenti qualsivoglia dato personale dovranno avvenire su sistemi che consentano la criptazione durante il trasporto dei dati (es. posta elettronica solo su POP3S/IMAPS/SMPTS)
4.4.6.	Normalizzazione struttura banca dati per esportazione e disponibilità del dato senza interruzioni/perdite, secondo gli standard.
4.4.7.	Nel caso di banche dati di tipo analogico, viene richiesta la distruzione delle stesse alla scadenza del contratto. **Qualora il fornitore abbia un obbligo di legge che determina la durata di conservazione delle banche dati analogiche, la distruzione dovrà essere garantita alla scadenza di tale obbligo di legge.**
4.4.8.	Nel caso di utilizzo di una VPN per accedere ai software e banche dati necessari per l'espletamento del servizio, tale connessione deve essere chiusa al termine della sessione di lavoro, al fine di evitare accessi non autorizzati e rischi alla sicurezza del Sistema Informativo del Comune di Olbia.
4.4.9.	Nel caso di **APP** per dispositivi mobili (*smartphone, tablet, etc.*) che richiedano una registrazione da parte di un utente/cittadino, dovrà essere garantita la dissociazione dai server del Fornitore, ossia deve essere annullata la registrazione e cancellati tutti i dati legati a tale registrazione una volta scaduto il contratto.
4.4.10.	Le funzionalità **di APP** idonee a consentire la tracciabilità dell'utente registrato, incluse quelle di geolocalizzazione mediante dispositivo mobile, dovranno prevedere specifici meccanismi di **acquisizione del consenso esplicito, libero e informato dell'utente**, ai sensi del Regolamento (UE) 2016/679 (GDPR).
4.4.11.	Nel caso vengano utilizzati sistemi ICT per la "Customer Satisfaction", deve essere garantito l'anonimato degli utenti che partecipano alla rilevazione. Tutte le relative elaborazioni analitiche dei dati devono essere consegnate all'amministrazione in formato digitale e completamente cancellate dai sistemi del fornitore una volta scaduto il contratto.
4.5.	**SITI e PORTALI**
4.5.1.	Eventuali Siti e Portali sviluppati ad-hoc che il Fornitore dovesse mettere a disposizione per contratto, durante il contratto devono rimanere sempre accessibile/modificabile da parte dell'Ente.
4.5.2.	Il Data Center dove risiede il server che ospiterà il Sito/Portale, di cui al punto 4.5.1., dovrà essere certificato ACN. Sarà onere del fornitore dare tutte le informazioni relative alle applicazioni informatiche utilizzate, comprese quelle della ditta fornitrice del software.
4.6.	**AI - ARTIFICIAL INTELLIGENCE**
4.6.1.	L'utilizzo da parte del Fornitore di strumenti di AI deve essere assolutamente concordato con il Comune di Olbia, attraverso parere del responsabile del Servizio ICT e del DPO dell'Ente. Gli eventuali strumenti di AI devono essere certificati ACN (*sia la componente software che il DataCenter dove girano applicazione e algoritmi*).
4.6.2.	Human-in-the-loop: ogni decisione che produca effetti giuridici per il contribuente deve essere validata da un funzionario umano. L'IA può segnalare l'anomalia, ma non può emettere l'atto autonomamente.
4.6.3.	Divieto di delega decisionale: il Fornitore deve garantire che i criteri di "scelta" degli algoritmi siano approvati preventivamente dal Comune.
4.6.4.	Spiegabilità (*Explainability*): La partecipata deve utilizzare modelli i cui output siano motivabili. Se un cittadino chiede perché è stato selezionato per un controllo, la risposta non può essere "lo ha deciso l'algoritmo".
4.6.5.	Conoscibilità del codice: È opportuno inserire clausole che permettano al Comune (*o ad autorità terze*) di ispezionare l'algoritmo per verificare l'assenza di bias (*discriminazioni sistematiche*)
4.6.6.	Sovranità dei dati: i dati devono risiedere su server europei o in cloud qualificati ACN.
4.6.7	Finalità limitata: è vietato l'uso dei dati raccolti per finalità diverse da quelle indicate nel contratto (*non possono essere usati per analisi di marketing turistico commerciale se non previo consenso esplicito e separato, etc.*).
4.6.8.	DPIA obbligatoria: il Fornitore deve condurre una Valutazione di Impatto sulla Protezione dei Dati (DPIA) specifica per l'uso dell'IA o dare motivazione sottoscritta digitalmente che la DPIA non è necessaria.

4.6.9.	Il Comune di Olbia deve restare proprietario dei dati elaborati e dei modelli di analisi generati attraverso strumenti di AI.
4.6.10.	Alla chiusura del contratto, il Fornitore, relativamente agli strumenti "AI" utilizzati, deve garantire la migrazione dei dati e dei modelli in formati aperti per evitare il "vendor lock-in".

Il Fornitore
Documento firmato digitalmente