POMPEII

PARCO
ARCHEOLOGICO
DI POMPEI

ISTITUTO
ITALIANO DI
TECNOLOGIA

ACCORDO N. 2
PER LO SVOLGIMENTO DEL PROGRAMMA DI RICERCA "Monitoraggio della conservazione del vetro antico

in attuazione della Convenzione Quadro stipulata in data 12/04/2023 (Prot. IIT n. 2683/23 del 04/04/2023, conv. PAP n. 18 del 13/04/2023) fra il *PARCO ACHEOLOGICO DI POMPEI* (di seguito "PAP") e la FONDAZIONE ISTITUTO ITALIANO DI TECNOLOGIA (di seguito "IIT")
di seguito denominate anche, singolarmente e/o congiuntamente, "la Parte" e/o "le Parti"

1. Titolo del Programma di Ricerca oggetto dell'Accordo
Monitoraggio della conservazione del vetro antico (Monitoring Ancient Glass – MAG).

2. Descrizione dettagliata del Programma di Ricerca
Il Programma di Ricerca prevede l'esposizione di 9 campioni replica di vetro antico in un ambiente destinato alla musealizzazione di oggetti archeologici sito nell'area del Parco Archeologico di Pompei. In particolare, le Parti hanno individuato di comune accordo nel Museo di Boscoreale (parte del PAP) una sede ideale per la sperimentazione.
Lo studio mira a monitorare l'effetto dell'ambiente sui processi di alterazione attivi su oggetti in materiale vetroso esposti. I dati ambientali (temperatura e umidità relativa) del luogo di esposizione verranno monitorati quotidianamente attraverso l'uso di un data logger e registrati per poter essere correlati alle condizioni di conservazione dei campioni esposti.
La durata totale del Programma di Ricerca è di 36 mesi, al termine dei quali i campioni verranno raccolti ed analizzati mediante appropriate tecniche di analisi. Dopo 1 anno di esposizione, una prima campagna di analisi verrà effettuata, in modo da comparare i risultati con quelli ottenuti al termine dei 36 mesi.
Lo studio fa parte di un progetto più ampio, portato avanti in parallelo in diversi Paesi Europei, nell'ambito del quale campioni replica identici a quelli che verranno esposti nel sito archeologico di Pompei verranno esposti contemporaneamente in diversi ambienti museali appartenenti a diverse aree climatiche.

3. Team di Ricerca
Per l'esecuzione del Programma di Ricerca ciascuna Parte individua un Responsabile Scientifico e il personale che prenderà parte alle attività di ricerca. I Responsabili avranno il compito di predisporre e definire nel dettaglio il Programma di Ricerca, nonché di valutare periodicamente e concordare eventuali aggiornamenti al piano di attività.

Per PAP:
- **Responsabile Scientifico:** *Alessandra Zambrano, funzionario ingegnere, Responsabile dell'Ufficio ricerca ed Innovazione*
- **Personale (dipendente, collaboratori e studenti) coinvolto:** *il gruppo di lavoro sarà definito con atto interno al PAP*

Per IIT:
- **Responsabile Scientifico:** *Arianna Traviglia, Dr., Coordinatrice CCHT*
- **Personale (dipendente e collaboratori di IIT, nonché eventuale personale affiliato a IIT) coinvolto:**
  Giulia Franceschin,

Roberta Zanini,
Mauro Moglianetti.

Ciascuna Parte ha facoltà di sostituire il Responsabile Scientifico e/o il personale coinvolto di propria indicazione mediante comunicazione scritta da inviare all'altra Parte con indicazione del nominativo del nuovo membro e di quello che si intende sostituire.

4. Durata del Programma di Ricerca e diagramma temporale

Il programma avrà una durata di tre (3) anni. Eventuali proroghe potranno venire concordate per iscritto fra le Parti.

Ogni 6 mesi: trasferimento dei dati di temperatura e umidità relativa dal data logger.
Al termine del 1 anno: prima campagna di analisi. Una parte dei campioni sarà inviata al laboratorio.
Al termine dei 3 anni: campagna di analisi conclusiva. I campioni rimanenti vengono inviati al laboratorio.

5.Laboratori/locali coinvolti nella collaborazione

Ad integrazione di quanto stabilito all'articolo 10 (Sicurezza e Ambiente) della Convenzione Quadro e ferma restando la responsabilità del datore di lavoro della Parte ospitante al rispetto della normativa vigente riguardante la conformità dei luoghi e delle attrezzature di lavoro di sua proprietà, le Parti si impegnano a:

- garantire la rispondenza dei propri locali, spazi e attrezzature, messi a disposizione per lo svolgimento delle attività previste dall'Accordo, con particolare riferimento alle disposizioni in materia di urbanistica, di salute e sicurezza sul lavoro, ambientale e di prevenzione incendi;
- garantire che le macchine, le attrezzature e le opere provvisionali ivi utilizzate e messe a disposizione dei lavoratori siano conformi alla normativa vigente e regolarmente soggette a verifica e manutenzione;
- garantire che i dispositivi di protezione individuale messi a disposizione dei lavoratori siano conformi ai requisiti previsti dalla normativa vigente e mantenuti in efficienza.

6. Impegni delle Parti

Ciascuna Parte, tenuto conto delle proprie disponibilità, sosterrà in autonomia i costi e le spese necessari per lo svolgimento delle attività di cui al Programma di Ricerca. In particolare, ciascuna Parte rimane esclusiva responsabile di: (i) la retribuzione del proprio personale coinvolto nel Programma di Ricerca, inclusi eventuali costi di trasferta, vitto ed alloggio; (ii) le spese connesse all'utilizzo dei propri laboratori, delle attrezzature e del materiale necessario allo svolgimento delle attività inerenti al Programma di Ricerca.
Le Parti danno espressamente atto che il trasferimento dei campioni replica di vetro romano oggetto del presente Programma di Ricerca avverrà nel rispetto di quanto previsto dall'art. 8 – "Trasferimento di materiali" della Convenzione Quadro ed utilizzando il modello facsimile di cui all'Allegato 2 della medesima.

7. Sicurezza delle Informazioni e dei dati personali

POMPEII

PARCO
ARCHEOLOGICO
DI POMPEI

ISTITUTO
ITALIANO DI
TECNOLOGIA

Ad integrazione di quanto disposto all'art. 13 e art. 14 della Convenzione Quadro, rubricati "Sicurezza delle Informazioni" e "Trattamento dei dati personali" le Parti si impegnano ad adottare le misure indicate agli allegati 1 e 2 del presente Programma di Ricerca.

8. Recesso e Risoluzione

8.1 Ciascuna Parte si riserva il diritto di recedere dal presente Accordo in ogni momento ed a suo insindacabile giudizio, mediante preavviso di 30 (trenta) giorni da comunicare all'altra Parte mediante lettera raccomandata A/R o tramite PEC.

8.2 Ciascuna Parte si riserva, altresì, il diritto di risolvere il presente Accordo in caso di inadempimento, da parte dell'altra Parte, di uno degli obblighi previsti dagli articoli 5 (Pubblicazioni), 6 (Obblighi di riservatezza), 7 (Gestione della proprietà intellettuale), 8 (trasferimento dei materiali), 9 (Garanzie), 10 (Sicurezza e ambiente), 13 (Sicurezza delle informazioni), 14 (Trattamento dei dati personali) e 15 (Gestione degli incidenti informatici e del Data Breach) della Convenzione Quadro, mediante lettera raccomandata A.R. o comunicazione a mezzo pec da notificare all'altra Parte con preavviso di 30 (trenta) giorni, salvo che la Parte inadempiente non provveda a sanare la propria situazione di inadempienza durante tale periodo di preavviso.

9. Rinvio

Resta inteso che, per quanto qui non espressamente previsto e/o richiamato, restano ferme le previsioni contenute nella Convenzione Quadro intervenuta tra le Parti e che, laddove non diversamente precisato, i termini utilizzati nel presente Accordo hanno lo stesso significato ad essi attribuito nella Convenzione Quadro.

Visto, approvato e sottoscritto digitalmente.

Parco Archeologico di Pompei	Fondazione Istituto Italiano di Tecnologia
Dott. Gabriel Zuchtriegel Direttore Generale	Prof. Giorgio Metta Direttore Scientifico

Firmato digitalmente da:
METTA GIORGIO
Data: 05/10/2023 09:25:29

Allegato 1: Misure di sicurezza tecnico-organizzative ICT
Allegato 2: Misure di sicurezza organizzative relative ai dati personali

Firmato digitalmente da
ZUCHTRIEGEL GABRIEL
JOHANNES
C: IT

POMPEII

PARCO
ARCHEOLOGICO
DI POMPEI

ISTITUTO
ITALIANO DI
TECNOLOGIA

ALLEGATO 1
MISURE DI SICUREZZA TECNICO-ORGANIZZATIVE ICT

1. MISURE DI SICUREZZA

Nelle tabelle di seguito riportate sono indicate le misure di sicurezza, divise in "organizzative" e "tecniche", la cui implementazione deve essere garantita a protezione delle informazioni in formato digitale trattate all'interno del Protocollo d'Intesa o degli ulteriori accordi che ne costituiscono attuazione da ciascuna Parte coinvolta per mezzo di un suo referente tecnico indicato nei paragrafi sottostanti.
Ciascuna Parte dovrà essere in grado, se richiesto dall'altra Parte, di fornire evidenza della conformità ai controlli selezionati. Nel caso in cui una Parte non sia in grado di soddisfare in tutto o in parte un obiettivo di controllo, è tenuta a segnalarlo all'altra Parte, fornendo le necessarie motivazioni e informazioni ed evidenza dei controlli compensativi rilevanti all'interno del presente allegato.
In caso di ricorso a fornitori (sub-responsabili) per la gestione dei servizi informatici e di sicurezza l'applicazione delle misure sotto descritte dovrà essere traferita contrattualmente ai fornitori stessi. Ciascuna Parte si impegna inoltre a tener traccia dei fornitori coinvolti in un registro apposito, che può essere richiesto dall'altra Parte per verifica e controllo.
Ogni qualvolta si verifichi un incidente di sicurezza che coinvolga le Informazioni trattate, questo dovrà essere comunicato tempestivamente ai referenti individuati nei paragrafi sottostanti, e comunque non entro le 24 ore successive all'evento nel caso l'incidente possa comportare una violazione di dati personali.

1.1. Misure di sicurezza organizzative

Item #	Categoria	Controllo	Compliance status IIT (S/N/n.a.)	Compliance status PAP (S/N/n.a.)	Note giustificative (se non applicabile, non implementato o parzialmente implementato, darne motivazione indicando i controlli compensativi applicati in sostituzione)

1	Policy di Sicurezza delle Informazioni	L'organizzazione deve documentare la propria politica per quanto riguarda l'elaborazione dei dati come parte della politica di sicurezza informatica. La politica di sicurezza deve essere riesaminata e riveduta, se necessario, su base annua. La politica di sicurezza deve almeno riferirsi a: ruoli e responsabilità del personale, le misure tecniche e organizzative di base adottate per la sicurezza dei dati, i responsabili dei dati o altre terze parti coinvolte nel trattamento di dati. La politica deve essere approvata dalla direzione e comunicata a tutti i dipendenti e alle parti esterne pertinenti.	S	S	
2	Ruoli e Responsabilità per la Sicurezza delle Informazioni	Deve essere identificato un responsabile della sicurezza delle informazioni, a cui devono essere comunicati i relativi compiti e responsabilità. Deve essere effettuata una chiara nomina dei responsabili aventi specifici compiti di sicurezza. Durante le re-organizzazioni interne o le cessazioni dei rapporti di lavoro o la modifica anche temporanea della mansione, la revoca dei diritti e delle responsabilità e le rispettive autorizzazioni devono essere definite chiaramente.	S	S	
3	Sicurezza delle Risorse Umane, Consapevolezza e Formazione	Prima iniziare il rapporto di lavoro ai dipendenti deve essere chiesto di prendere visione del documento o della politica di sicurezza dell'organizzazione e di firmare i rispettivi accordi di riservatezza e di non divulgazione. L'organizzazione deve avere programmi di formazione e sensibilizzazione strutturati e regolari per il personale, compresi programmi specifici relativi alla protezione dei dati. Il piano di formazione deve essere preparato ed eseguito su base annua, o con altra periodicità ritenuta adeguata.	S	S	
4	Policy di gestione degli asset	L'organizzazione deve documentare la propria politica per quanto riguarda l'utilizzo delle risorse informatiche aziendali.	S	S	
5	Policy di gestione dei dispositivi portatili	Devono essere definite e documentate delle policy e procedure per la gestione e l'uso corretto dei dispositivi mobili, comprendenti l'utilizzo o meno di	S	S	

		dispositivi personali e l'utilizzo di dispositivi aziendali per usi personali, e la definizione di ruoli specifici e responsabilità per quanto riguarda la gestione dei dispositivi mobili.			
6	Policy per il Controllo degli Accessi	Autorizzazioni specifiche per il controllo dell'accesso ai dati devono essere assegnate a ciascun ruolo in seguito alla necessità del rispetto del principio del "need to know". I criteri di controllo accesso devono essere dettagliati e documentati. L'organizzazione deve determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per ruoli utente specifici verso i processi e le procedure relative ai dati trattati. Il principio della "Segregation of Duty" (ad es. richiesta di accesso, autorizzazione di accesso, amministrazione dell'accesso) deve essere chiaramente definito e documentato.	S	S	
7	Procedure operative e responsabilità	Deve essere definita e aggiornata regolarmente una politica per la gestione dei cambiamenti che deve includere: un processo per l'introduzione di modifiche, i ruoli/utenti che hanno diritti di cambiamento, le timeline per l'introduzione di modifiche, la tracciatura delle modifiche e il loro monitoraggio. Deve essere svolto un controllo periodico di questo processo.	n.a.	n.a.	
8	Gestione degli incidenti relativi alla sicurezza delle informazioni	Deve essere definito e documentato un piano di risposta agli incidenti con procedure dettagliate per garantire una risposta efficace e ordinata agli incidenti. Il piano deve assicurare che le violazioni dei dati personali siano immediatamente segnalate al Titolare entro gli accordi contrattualizzati.	S	S	
9	Continuità della sicurezza delle informazioni	Deve essere dettagliato e documentato un Piano di Continuità operativa che preveda azioni ben definite e l'assegnazione dei ruoli. Nel piano deve essere definito un livello di qualità del servizio per i processi aziendali che forniscono servizi critici per la protezione dei dati. Deve essere identificato e nominato personale specifico con la responsabilità necessaria, l'autorità e	n.a.	n.a.	

		la competenza per gestire la continuità aziendale in caso di incidente/violazione dei dati personali. Una struttura alternativa deve essere considerata, a seconda dell'organizzazione e del tempo di inattività accettabile del sistema IT.			
10	Conformità alla sicurezza delle informazioni	L'organizzazione deve svolgere con cadenza almeno annuale una verifica (o audit interno) delle proprie misure tecniche e organizzative per l'implementazione di eventuali azioni correttive.	S	S	

1.2. Misure di sicurezza tecniche

ID	**Categoria**	**Controllo**	**Compliance status IIT** (S/N/n.a.)	**Compliance status PAP** (S/N/n.a.)	**Note giustificative** (se non applicabile, non implementato o parzialmente implementato, darne motivazione indicando i controlli compensativi applicati in sostituzione)
1	Gestione degli accessi e delle credenziali	Devono essere applicate misure di sicurezza agli accessi logici, come password robuste (o equivalente codice di protezione per dispositivi mobili) e modifica periodica delle stesse. Deve essere effettuata una revisione periodica dei permessi di accesso, ad esempio in caso di cessazione del rapporto con la Società o di cambiamenti interni all'organizzazione.	S	S	n.a. datalogger
2	Firewall	Deve essere attivato un firewall di rete, che permetta solo il traffico e i servizi necessari.	S	S	n.a. datalogger
3	Inventario	Gli asset gestiti (incluse le applicazioni) devono essere registrati in un inventario con le loro informazioni di rilievo, e aggiornati con periodicità non maggiore a 6 mesi.	S	S	n.a. datalogger
4	Patching	Devono essere usate versioni supportate di applicazioni e sistemi operativi. Le patch di sicurezza classificate come "critiche" e "gravi"	S	S	n.a. datalogger

		devono essere applicate entro 20 giorni dal rilascio, tutte le altre entro 90 giorni.			
5	Protezione da Malware	Deve essere installato e tenuto aggiornato un agente antivirus/anti-malware.	S	S	n.a. datalogger
6	Gestione delle vulnerabilità	Deve essere effettuata una scansione di vulnerabilità almeno ogni 3 mesi e le vulnerabilità ad alto rischio riscontrate devono essere risolte entro 10 giorni.	S	S	n.a. datalogger
7	Backup	Deve essere effettuato un backup almeno settimanale di dati e configurazioni. I dati di backup devono essere cifrati in transito e quando salvati su supporti esterni, e testati regolarmente per assicurarsi che possano essere usati in caso di necessità.	n.a	n.a.	
8	Sicurezza delle Comunicazioni	Le informazioni trasferite su canali applicativi devono essere cifrate nel trasporto, ad esempi usando protocolli sicuri (TLS, https, ssh) o canali cifrati (VPN).	S	S	n.a. datalogger
9	Cancellazione sicura	Quando non più necessari, i dati devono essere rimossi in maniera permanente con tecniche di cancellazione sicura. Per i device remoti, ciò deve poter essere controllato centralmente.	S	S	n.a. datalogger
10	Cifratura	Deve essere prevista la cifratura delle unità d'archiviazione, quali dischi rigidi (in particolare dei laptop), dischi e chiavette USB, DVD, backup tapes, ecc. Per i file, i record o i campi più critici devono essere considerate soluzioni di cifratura, adottandole ove possibile.	S	S	n.a. datalogger
11	Gestione dei log	I log, inclusi quelli degli Amministratori di Sistema, devono essere inviati ad un sistema di raccolta centrale, che ne prevenga l'alterazione. Per le applicazioni cloud, tali log devono essere resi disponibili ed esportati su richiesta entro 5 giorni.	S	S	n.a. datalogger
12	Sicurezza fisica	Le server room e i datacenter devono essere ad accesso controllato e provviste di misure di sicurezza fisica (antincendio, antiallagamento, controllo della temperatura, continuità elettrica).	n.a.	n.a.	

13	Revisione degli aspetti di Sicurezza, di Privacy e Legali	Deve essere eseguita una verifica degli aspetti di security, privacy e legali ed implementate le raccomandazioni conseguenti prima dell'utilizzo in produzione di applicazioni che trattano dati personali.	S	S	n.a. datalogger
14	Sviluppo di software sicuro	Lo sviluppo sicuro deve avvenire secondo i principi di privacy-by design e security-by-design. In particolare, gli ambienti di test devono essere separati dagli ambienti di produzione e non devono utilizzare dati reali.	n.a.	S	
15	Autenticazione forte	Deve essere implementato un sistema di autenticazione a 2 fattori per accessi degli amministratori di sistema e per tutti gli accessi a sistemi utilizzati per il trattamento di dati genetici o qualificati come "a maggior tutela".	S	S	n.a. datalogger

1.3. Referente informatico di PAP verso IIT

Per informazioni sulle checklist dei controlli di sicurezza organizzativi e tecnici, IIT può fare riferimento a:
Raffaele Martinelli
raffaele.martinelli@cultura.gov.it
+39 081 8575302

1.4. Referente tecnico di IIT verso PAP

Per informazioni sulle checklist dei controlli di sicurezza organizzativi e tecnici, PAP può fare riferimento a:

Contatto primario:
Supporto ICT
ict_servicedesk@iit.it

Contatto secondario:
Stefano Bencetti (ICT Director)
stefano.bencetti@iit.it
+39 010 2896 505

POMPEII

PARCO
ARCHEOLOGICO
DI POMPEI

ISTITUTO
ITALIANO DI
TECNOLOGIA

ALLEGATO 2

MISURE DI SICUREZZA ORGANIZZATIVE RELATIVE AI DATI PERSONALI

2. MISURE DI SICUREZZA ORGANIZZATIVE

Nella tabella di seguito riportata sono indicate le misure di sicurezza organizzative relative ai dati personali previste da IIT ai sensi del Regolamento Generale sulla protezione dei dati personali n. 679/2016 e s.m.i. (di seguito "GDPR"), per cui si richiede a XXX la dimostrazione della conformità attraverso la compilazione della colonna "Compliance Status Partner".

Nel caso in cui XXX non sia in grado di soddisfare in tutto o in parte i requisiti richiesti, è tenuto a specificarne la motivazione nella colonna "Note giustificative".

2.1. Misure di sicurezza organizzative

Item #	Categoria	Controllo	Compliance status IIT (S/N/n.a.)	Compliance status PAP (S/N/n.a.)	Note giustificative (se non applicabile, non implementato o parzialmente implementato, darne motivazione indicando i controlli compensativi applicati in sostituzione)
1	Analisi dei rischi	È stata effettuata l'analisi dei rischi e sono stati definiti ed implementati gli action plan per l'adeguamento delle misure di sicurezza organizzative (laddove necessario). L'analisi dei rischi viene costantemente aggiornata.	S	S	
2	Attribuzione di funzioni e compiti a soggetti autorizzati	Il personale interno che tratta dati personali è designato con apposito atto di nomina.	S	S	

3	Istruzioni al personale interno autorizzato al trattamento dei dati personali	Comunicazione di apposite istruzioni scritte al personale interno autorizzato al trattamento dei dati personali.	S	S	
4	Canale dedicato per la notifica delle violazioni di Dati Personali (se applicabile)	È disponibile un apposito canale per la comunicazione delle eventuali violazioni degli obblighi in tema di trattamento di Dati Personali.	S	S	
5	Designazione del Responsabile della Protezione dei Dati (se applicabile)	È designato un Responsabile della Protezione dei Dati a cui è affidato il compito di valutare ed organizzare la gestione del trattamento dei dati personali.	S	S	
6	Pseudonimizzazione dei dati personali (laddove applicabile):	Applicazione di misure di de-identificazione dei dati personali, in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive. Le informazioni aggiuntive sono conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.	S	S	

2.2. Referente GDPR di PAP verso IIT

Per informazioni sulla checklist dei controlli di sicurezza organizzativi, IIT può fare riferimento a:

Gabriel, Zuchtriegel
gabriel.zuchtriegel@cultura.gov.it
+39 081 8575300

2.3. Referente GDPR di IIT verso PAP

Per informazioni sulla checklist dei controlli di sicurezza organizzativi, PAP può fare riferimento a:

GDPR Team
gdpr@iit.it
+39 010 28961