

CAPITOLATO SPECIALE DESCRITTIVO E PRESTAZIONALE

Procedura aperta ai sensi dell'art. 71 del D.Lgs. n. 36/2023 per l'affidamento della fornitura e installazione del revamping parziale del sistema di controllo accessi e manutenzione, in favore della Fondazione Human Technopole.

CIG B5188D5FF1

Sommario

PREMESSA.....	3
Definizioni	4
1. DURATA E IMPORTO DELL'APPALTO	5
2. OGGETTO DELL'APPALTO	5
2.1 Revamping sistema di controllo accessi.....	5
Modello di riferimento del sistema controllo accessi da implementare	8
Caratteristiche Tecniche Minime Controllo Accessi	8
Compatibilità	9
2.2 Adeguamento dell'interfaccia con SW di gestione presenze Zucchetti Presenze Project.....	9
2.3 Adeguamento e integrazione degli impianti antintrusione in essere.....	10
Modello di riferimento del sistema antintrusione da integrare	11
Caratteristiche Tecniche Minime Antintrusione	12
Compatibilità	12
2.4 Realizzazione dell'impianto antintrusione Incubators IN1, IN2.....	12
Modello di riferimento del sistema antintrusione Incubators IN1, IN2, da realizzare	13
Caratteristiche Tecniche Minime Antintrusione	14
Compatibilità	15
2.5 Accessori e ricambi.....	15
2.6 Assistenza	16
3 REQUISITI.....	17
3.1 Requisiti tecnico-professionali	17
3.2 Requisiti ICT	17
4. ALTRI SERVIZI.....	19
4.1. COLLAUDO	19
4.2. GARANZIA	19
5. MODALITA' DI ESECUZIONE DELL'APPALTO.....	20
5.1. Modalità di fornitura e installazione	20
5.2. Piano di realizzazione	20

5.3. Sopralluogo ispettivo.....	20
6. TEMPISTICHE DI ESECUZIONE DELL'APPALTO	21
6.1. Modalità di consegna.....	21
7. TRATTAMENTO E TUTELA DEI DATI PERSONALI.....	21

PREMESSA

Il presente Capitolato Speciale Descrittivo e Prestazionale disciplina le caratteristiche tecniche della fornitura di un **revamping parziale del sistema di controllo accessi oltre che del sistema antintrusione** da installarsi presso gli edifici e il datacenter della Fondazione Human Technopole, inclusiva di tutti i servizi annessi meglio specificati nelle successive sezioni quali: montaggio hardware, cablaggi, configurazioni, redazione di documenti, collaudo, garanzia hardware e software.

L'attuale impianto controllo accessi del campus è composto da 4 sottosistemi indipendenti basati su diverse tecnologie di lettura, rispettivamente:

- PIT – Lenel OnGuard (MIFARE)
- NPA – Siemens (MIFARE)
- SPA (main entrance) – Zucchetti (MIFARE)
- INC – Vanderbilt (125Khz)

integrati ai minimi comuni livelli di funzionalità dal sistema ADITUM Web.

L'attuale impianto antintrusione è composto da 3 sistemi separati, rispettivamente:

- PIT – Lenel OnGuard
- NPA – Siemens
- SPA – Schneider
- INC – (NON INSTALLATO)
- IN3 – (Lenel OnGuard IN CORSO DI INSTALLAZIONE)

Le attività richieste riguardano:

1) il revamping parziale dei sistemi di controllo accessi nel sistema integrato di controllo accessi e antintrusione in essere presso la Fondazione Human Technopole Palazzo Italia (PIT), sui seguenti edifici:

- North Pavilion (NPA)
- South Pavilion (SPA)
- Incubators (INC): Incubator 1 (IN1) - Incubator 2 (IN2) - Incubator 3 (IN3)

2) Adeguamento dell'interfaccia con SW di gestione presenze Zucchetti Presenze Project

3) l'integrazione degli impianti antintrusione nel sistema integrato di controllo accessi e antintrusione in essere presso la Fondazione Human Technopole Palazzo Italia (PIT), sui seguenti edifici:

- North Pavilion (NPA)
- South Pavilion (SPA)
- Incubators (INC): Incubator 3 (IN3)

4) la realizzazione dell'impianto antintrusione nel sistema integrato di controllo accessi e antintrusione in essere presso la Fondazione Human Technopole Palazzo Italia (PIT), sui seguenti edifici:

- Incubators (INC): Incubator 1 (IN1) - Incubator 2 (IN2)

Definizioni

Le seguenti **sigle** sono utilizzate nel prosieguo del documento:

Termine o sigla	Definizione
PIT	Edificio Palazzo Italia
NPA	Edificio North Pavilion
SPA	Edificio South Pavilion
INC o INx (IN1, IN2, IN3)	Edifici Incubators (Incubator 1, Incubator 2, Incubator 3)
KHz	Kilo Hertz
MHz	Mega Hertz
GHz	Giga Hertz
MIFARE	chip usato nelle smart card contactless e nelle carte di prossimità. Include soluzioni basate su diversi livelli della ISO/IEC 14443 Type-A 13.56MHz contactless smart card standard.
IP	Internet Protocol
I/O	Input / Output
SW	Software
HW	Hardware

Le seguenti **definizioni** sono utilizzate nel prosieguo del documento:

Termine o sigla	Definizione
Produttore o Costruttore	Costruttore degli apparati HW e/o proprietario dei diritti intellettuali del SW compresi nell'offerta.
Fornitore	Partecipante alla trattativa
FHT	Fondazione Human Technopole

1. DURATA E IMPORTO DELL'APPALTO

La durata massima del contratto sarà di 65 mesi a partire dalla data di sottoscrizione o del verbale di avvio ove precedente, di cui massimo n. 5 mesi per la fornitura, realizzazione delle opere e collaudo (fatte salve eventuali necessità di prolungamento dei tempi della stazione appaltante oltre al 5° mese), oltre a 24 mesi di manutenzione e assistenza a decorrere dalla data di collaudo ed ulteriori 36 mesi di manutenzione e assistenza opzionali.

Il valore complessivo stimato dell'appalto comprensivo delle opzioni /rinnovi previsti ai sensi dell'art. 120 del Codice, al netto di IVA è pari ad **€ 627.600,00 (euro seicentoventisettemilaseicento/00)**, così suddivisi:

€ 331.000,00 (euro trecentotrentunomila/00) I.V.A. esclusa, a copertura della fornitura e posa in opera, ivi compresa la configurazione dei sistemi, e collaudo e ai primi 24 mesi di manutenzione, di cui:

- Revamping Controllo Accessi e Antintrusione € 205.000,00
- Manutenzione a canone € 40.000,00
- Licenze € 16.000,00
- Ricambi originali extra € 40.000,00
- Interventi manutentivi extra canone € 30.000,00

Gli importi di cui sopra comprendono:

- gli oneri da interferenza sono pari a 2.814,92 €
- il costo della manodopera si stima in un importo pari a 60.500,00 €

€ 192.000,00 (euro centonovantaduemila/00) I.V.A. esclusa, di manutenzione opzionale triennale e assistenza (3y), così suddivisi:

- Manutenzione a canone € 63.000,00
- Licenze 24.000,00
- Ricambi originali extra € 60.000,00
- Interventi manutentivi extra canone € 45.000,00

€ 104.600,00 (euro centoquattromilaseicento/00) quale importo massimo per l'eventuale quinto d'obbligo, per i quali verranno emesse a budget apposite coperture in considerazione dei servizi effettivamente da attivarsi.

Gli importi di cui sopra comprendono:

- gli oneri da interferenza sono pari a 3.890,4 €
- il costo della manodopera si stima in un importo pari a 28.500,00 €

2. OGGETTO DELL'APPALTO

2.1 Revamping sistema di controllo accessi

La fornitura consta delle seguenti attività di dettaglio per ciascun building, la fornitura dei componenti, nella numerosità **minima, a pena di esclusione**, indicata e di seguito ulteriormente specificata, è da intendersi comprensiva dei servizi connessi.

Palazzo Italia PIT	
Quantità	Tipologia
1	Aggiornamento versioning delle licenze in uso da v 7.5 a 8.1 o superiore
1	Migrazione su nuovo server messo a disposizione dalla committente
3	Licenze SW per postazione PC Client
1	Bundle licenze 64 lettori badge
1	Sviluppo file I/O per invio ricorrente transiti (presenze) a sistema paghe Zucchetti tramite agent dedicato
1	Inserimento e configurazione mappe grafiche per tutti i varchi PIT
1	Creazione report
1	Workstation completa di: <ul style="list-style-type: none"> n. 1 PC tower (opportunamente dimensionato per i requisiti consigliati dal sistema installato), e con le seguenti caratteristiche minime: <ul style="list-style-type: none"> Processore i5 Min. 16 GB RAM 1 disco SSD da min. 512GB Scheda video dedicata min 4GB OS Win10Pro n. 2 monitor min. 27" per utilizzo H24 n. 1 supporto da scrivania per 2 monitor sovrapposti n. 1 Tastiera e mouse Estensione del service care e garanzia del produttore per min. 3 anni. UPS locale per protezione della postazione per min. 15 minuti

Incubator 3 IN3	
Quantità	Tipologia
1	Inserimento e configurazione mappe grafiche per tutti i varchi IN3
1	Creazione report

North Pavilion NPA	
Quantità	Tipologia
2	Controller OSDP 32 varchi espandibile
2	Box alimentatore supervisionato 12V8A/24V4A con batteria tampone
20	Scheda di controllo varco bidirezionale
21	Lettore badge OSDP mobile enabled (tipo HID Signo 20)
6	Scheda 4 fusibili supervisionata per protezione elettroserratura
20	Ricablaggio serrature elettriche e pulsanti uscita esistenti

Planimetrie: Rif. Annex 1 – 1.1 Planimetria Controllo Accessi North Pavilion NPA

South Pavilion SPA	
Quantità	Tipologia
1	Controller OSDP 32 varchi espandibile
1	Box alimentatore supervisionato 12V8A/24V4A con batteria tampone
1	Scheda di controllo varco bidirezionale
2	Lettore badge OSDP mobile enabled (tipo HID Signo 20)
1	Scheda 4 fusibili supervisionata per protezione elettroserratura
1	Ricablaggio serratura elettrica

Planimetrie: Rif. Annex 1 – 1.1 Planimetria Controllo Accessi South Pavilion SPA

Incubator 1 IN1	
Quantità	Tipologia
1	Controller OSDP 32 varchi espandibile
1	Box alimentatore supervisionato 12V8A/24V4A con batteria tampone
5	Scheda di controllo varco bidirezionale
10	Lettore badge OSDP mobile enabled (tipo HID Signo 20)
2	Scheda 4 fusibili supervisionata per protezione elettroserratura
5	Ricablaggio serratura elettrica

Planimetrie: Rif. Annex 1 – 1.1 Planimetria Controllo Accessi Incubator 1 IN1

Incubator 2 IN2	
Quantità	Tipologia
1	Controller OSDP 32 varchi espandibile
1	Box alimentatore supervisionato 12V8A/24V4A con batteria tampone
2	Scheda di controllo varco bidirezionale
3	Lettore badge OSDP mobile enabled (tipo HID Signo 20)
1	Scheda 4 fusibili supervisionata per protezione elettroserratura
2	Ricablaggio serrature elettriche e pulsanti uscita esistenti

Planimetrie: Rif. Annex 1 – 1.1 Planimetria Controllo Accessi Incubator 2 IN2

Servizi connessi:

- Sopralluogo tecnico-operativo successivo all'aggiudicazione della gara, atto a definire nel dettaglio le modalità di installazione e realizzazione (a titolo esemplificativo e non esaustivo il posizionamento di elementi di campo quali controller e lettori, la priorità di realizzazione di porzioni di impianto rispetto ad altre);
- Fornitura e posa in opera dell'hardware, di predisposizioni elettriche e cavidrettoria;
- Licenze;
- Montaggio e cablaggio;
- Collegamento e cablaggio a rete elettrica e rete dati;
- Installazione e configurazione software;
- Raccolta di anagrafiche, gruppi, utenze e profili dell'impianto esistente e importazione nel nuovo impianto;
- Configurazione funzione di evacuazione in caso di emergenza e relativi totem punto di raccolta;
- Inserimento e configurazione mappe grafiche;
- Integrazione logiche antintrusione e controllo accessi sui varchi;
- Adeguamenti per integrazione dati presenze mediante generazione del file per interfaccia con software di gestione paghe Zucchetti HR Workflow (tramite agent dedicato);
- Collaudo e verifica delle prestazioni;
- Training per operatori;
- Redazione file DWG e documentazione tecnica as built
- Garanzia e Assistenza.

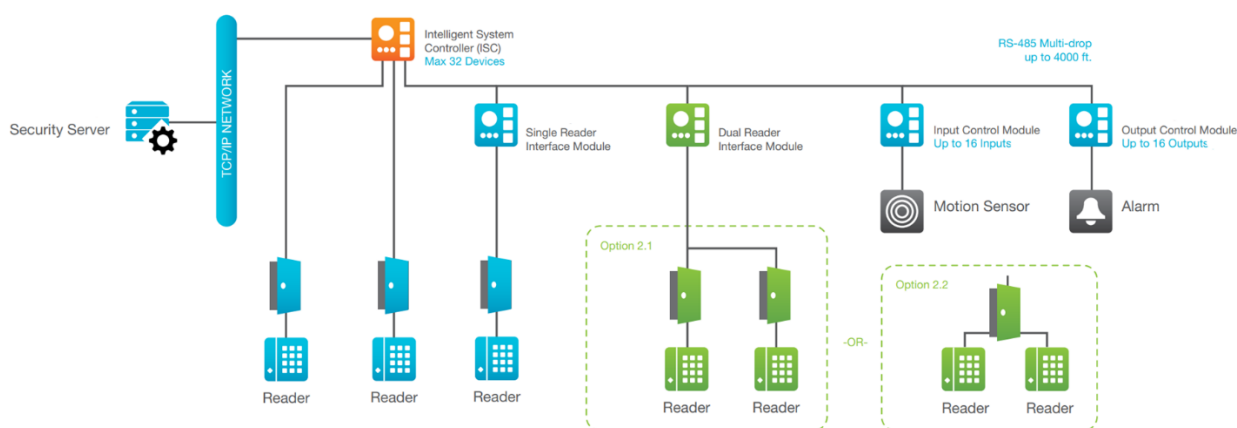
La fornitura deve inoltre comprendere eventuali altri componenti e servizi, **anche se non esplicitamente menzionati**, ma comunque necessari per la gestione, l'integrazione e il corretto funzionamento del sistema all'interno dell'infrastruttura esistente di Fondazione Human Technopole, in seguito abbreviato come FHT (ad esempio i cavi di collegamento o di alimentazione).

Si precisa che, alla data di presentazione dell'offerta nessuna delle componenti hardware della soluzione proposta deve essere stata dichiarata End-Of-Life dal costruttore, pena l'esclusione dalla procedura di gara.

La fornitura deve essere costituita **esclusivamente da materiale nuovo di fabbrica**. Sono pertanto vietati elementi (sia macro che micro, sia singoli che in gruppo, sia interni che esterni) ricondizionati, refurbished, dimostrativi, provenienti da canali di brokeraggio, da campionari, da fiere, da esposizione, da test interni o in visione presso clienti e in generale tutto ciò che non sia al primo utilizzo.

Modello di riferimento del sistema controllo accessi da implementare

Di seguito l'architettura del sistema di controllo accessi e antintrusione integrato.



L'installazione del controller deve avvenire lasciando libere le due uscite dirette verso i varchi per garantire immediata scalabilità dell'impianto. Ogni controller deve avere un box alimentazione con batteria tampone, l'installazione deve essere effettuata per quanto possibile nei locali tecnici più prossimi alla zona e ad altezza uomo, evitando l'installazione nei controsoffitti e nei sottopavimenti.

Ogni varco, indipendentemente sia IN oppure IN/OUT deve essere connesso ad una scheda di controllo varco bidirezionale (Dual reader interface module) dedicata.

Per ogni varco protetto da controllo accessi, occorre collegare il contatto magnetico (laddove presente) alla scheda di controllo varco, al fine di rilevare eventuali tentativi di forzatura del varco.

Laddove presente, oltre al ricablaggio della serratura elettrica, occorre prevedere il ricablaggio del pulsante di uscita.

Fermo restando le caratteristiche minime descritte, il fornitore potrà proporre eventuali variazioni che riterrà migliorative (in termini di funzionalità, semplicità, ridondanza, ecc.), eventuali variazioni saranno comunque oggetto di valutazione e accettazione da parte della stazione appaltante.

Caratteristiche Tecniche Minime Controllo Accessi

#	Caratteristiche Tecniche Minime	Val. min.
Controller		
1	Memoria flash non volatile disponibile a bordo	6 MB

2	Storage eventi con batteria tampone	50.000
3	Connessione di device via RS-485	32
4	Compatibilità con lettori OSDP	Si
5	Ingressi input	8
6	Supervisione contatto porta (aperto/chiuso)	Si
Box alimentatore supervisionato 12V8A/24V4A con batteria tampone		
1	Tamper anteriore e posteriore	Si
2	Output selezionabile 13.8 V / 27.6 VDC	Si
3	Supporti guida cavi	Si
4	Piastre di espansione	2
Scheda di controllo varco bidirezionale		
1	Lettori gestiti	2
2	Supervisione contatto porta (aperto/chiuso)	Si
3	Compatibilità con lettori OSDP	Si
4	Contatti input	8
5	Contatti output	6
Lettore badge OSDP mobile enabled (tipo HID Signo 20)		
1	Compatibilità OSDP	Si
2	Multitecnologia, mobile ready (bluetooth e NFC)	Si
3	Frequenza	13.56 MHz, e 2.4 GHz
4	Adatto per installazione su montante porta	Si

Compatibilità

Si richiede che il materiale fornito abbia le seguenti certificazioni:

- Controllo Accessi: OSDP, compatibile con sistema in essere presso PIT
- Lettori badge: OSDP, mobile enabled, compatibile con sistema in essere presso PIT

I sistemi forniti non devono contenere componenti o dispositivi che non siano compatibili con il sistema integrato di controllo accessi e antintrusione installato presso Palazzo Italia.

È richiesto che il fornitore produca un foglio di calcolo in formato Excel in cui saranno indicati tutti i riferimenti identificativi della componente HW (es. S/N, MAC address, ecc.) e dei riferimenti di rete (elettrica, dati) a cui questa è connessa.

2.2 Adeguamento dell'interfaccia con SW di gestione presenze Zucchetti Presenze Project

L'attuale integrazione prevede che dal sistema di controllo accessi in uso venga generato un file chiamato TIMBRA.TXT contenente tutti i transiti della giornata e aggiornato in tempo reale.

Ad un orario specifico pre-impostato, l'Agent Zucchetti dedicato installato sul server, preleva le informazioni svuotando il file e le invia allo studio paghe secondo dei parametri impostati nei settaggi dell'Agent stesso. Una copia del file contenente tutti i transiti inviati e con naming indicante anche data e ora dell'export viene archiviato per backup in apposita cartella.

A seguito dell'invio, il file TIMBRA.TXT si ripopola con i nuovi transiti di volta in volta effettuati.

A titolo indicativo si riporta di seguito struttura tipo del file TIMBRA.TXT:

xx	ID Badge	Data	Ora	Ingresso / Uscita	Cod. varco	xx	xx
----	----------	------	-----	-------------------	------------	----	----

01	000000000000123	18/04/24	12:41	I	00045	00	P
01	000000000000456	18/04/24	12:52	U	00078	00	P

Occorre realizzare un nuovo file riportante le medesime informazioni, con la medesima periodicità oraria di invio e le medesime modalità di archiviazione dello storico transiti in produzione.

Nel server di controllo accessi andrà installato l'agent Zucchetti dedicato opportunamente settato per invio dei dati allo studio paghe.

2.3 Adeguamento e integrazione degli impianti antintrusione in essere

La fornitura consta delle seguenti attività di dettaglio per ciascun building, la fornitura dei componenti, nella numerosità **minima, a pena di esclusione**, indicata e di seguito ulteriormente specificata, ed è da intendersi comprensiva dei servizi connessi.

Palazzo Italia PIT	
Quantità	Tipologia
1	Configurazione server
1	Configurazione mappe grafiche e zone per tutti i sensori (PIT, NPA, SPA, INx)
1	Riattivazione impianto e settaggio sensori di campo PIT

Incubator 3	
Quantità	Tipologia
1	Configurazione mappe grafiche e zone per tutti i sensori (IN3)
1	Riattivazione impianto e settaggio sensori di campo IN3

North Pavilion NPA	
Quantità	Tipologia
Min. 4	Box alimentatore supervisionato 12V8A/24V4A con batteria tampone
6	Scheda di controllo input 16 contatti
6	Scheda di controllo output 16 contatti
1 (tutti)	Ricablaggio di tutti i sensori di campo esistenti (input e output)

Planimetrie: Rif. Annex 1 – 1.2 Planimetria Antintrusione North Pavilion NPA

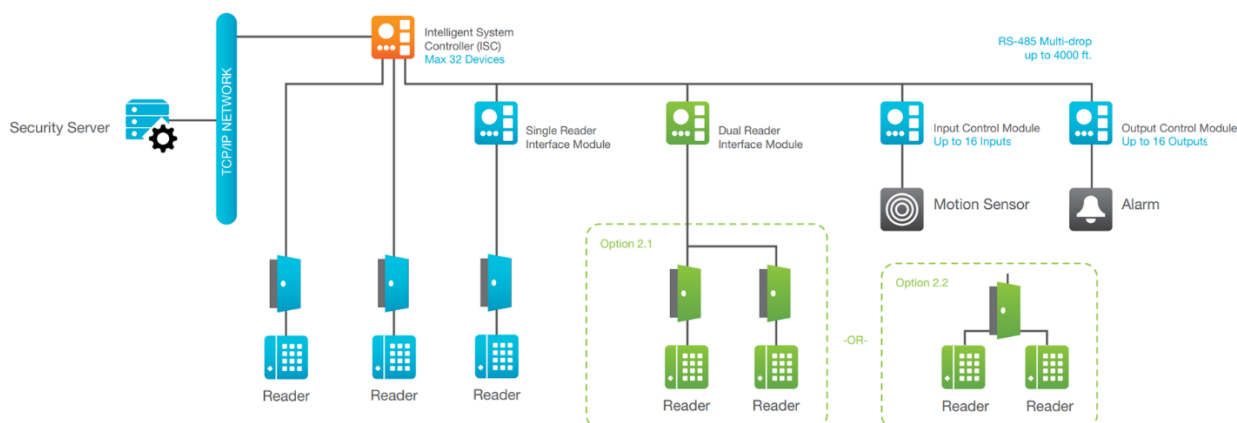
South Pavilion SPA	
Quantità	Tipologia
Min. 6	Box alimentatore supervisionato 12V8A/24V4A con batteria tampone
10	Scheda di controllo input 16 contatti

6	Scheda di controllo output 16 contatti
1 (tutti)	Ricablaggio di tutti i sensori di campo esistenti (input e output)

Planimetrie: Rif. Annex 1 – 1.2 Planimetria Antintrusione South Pavilion SPA

Modello di riferimento del sistema antintrusione da integrare

Di seguito l'architettura del sistema antintrusione integrato nel sistema di controllo accessi.



L'installazione dei concentratori (box alimentazione + schede di controllo I/O) deve avvenire per quanto possibile in punti distribuiti omogeneamente a garantire la copertura dell'edificio lasciando liberi almeno 4 contatti INPUT e OUTPUT in ogni concentratore per garantire immediata scalabilità dell'impianto.

Ogni punto di concentratori deve essere costituito da un box alimentazione con batteria tampone, e un numero sufficiente di schede di controllo input e output per coprire tutti i sensori di campo della zona sia di INPUT (es. contatti magnetici, volumetrici, ecc.) che di OUTPUT (es. sirene da interno o esterno) l'installazione deve essere effettuata per quanto possibile nei locali tecnici più prossimi alla zona e ad altezza uomo, evitando l'installazione nei controsoffitti e nei sottopavimenti. Laddove non fosse possibile effettuare l'installazione nei locali tecnici, è preferibile identificare aree coperte da videosorveglianza e non raggiungibili ad altezza uomo.

Il fornitore potrà proporre eventuali variazioni che riterrà migliorative (in termini di ottimizzazione dell'impianto, semplicità, ridondanza, ecc.), eventuali variazioni saranno comunque oggetto di valutazione e accettazione da parte della stazione appaltante.

Servizi connessi:

- Sopralluogo tecnico-operativo successivo all'aggiudicazione della gara, atto a definire nel dettaglio le modalità di installazione e realizzazione (a titolo esemplificativo e non esaustivo il posizionamento di elementi di campo quali concentratori e sensori, la priorità di realizzazione di porzioni di impianto rispetto ad altre);
- Fornitura e posa in opera dell'hardware, di predisposizioni elettriche e cavi;
- Licenze;
- Montaggio e cablaggio;
- Collegamento ed eventuale adattamento cablaggio dei sensori campo INPUT e OUTPUT;
- Collegamento e cablaggio a rete elettrica e rete dati;

- Installazione e configurazione software;
- Riconfigurazione e settaggio di tutti i sensori antintrusione in campo presso PIT, NPA, SPA e IN3;
- Inserimento e configurazione mappe grafiche nel sistema integrato;
- Configurazione delle logiche antintrusione (zone, fasce orarie, ecc.);
- Collaudo e verifica delle prestazioni;
- Training per operatori;
- Redazione file DWG e documentazione tecnica as built;
- Garanzia e Assistenza.

La fornitura deve inoltre comprendere eventuali altri componenti e servizi, **anche se non esplicitamente menzionati**, ma comunque necessari per la gestione, l'integrazione e il corretto funzionamento del sistema all'interno dell'infrastruttura esistente di Fondazione Human Technopole, in seguito abbreviato come FHT (ad esempio i cavi di collegamento o di alimentazione).

Si precisa che, alla data di presentazione dell'offerta nessuna delle componenti hardware della soluzione proposta deve essere stata dichiarata End-Of-Life dal costruttore, pena l'esclusione dalla procedura di gara.

La fornitura deve essere costituita **esclusivamente da materiale nuovo di fabbrica**. Sono pertanto vietati elementi (sia macro che micro, sia singoli che in gruppo, sia interni che esterni) ricondizionati, refurbished, dimostrativi, provenienti da canali di brokeraggio, da campionari, da fiere, da esposizione, da test interni o in visione presso clienti e in generale tutto ciò che non sia al primo utilizzo.

Caratteristiche Tecniche Minime Antintrusione

#	Caratteristiche Tecniche Minime	Val. min.
Scheda di controllo input 16 contatti		
1	Contatti input	16
2	Input dedicato a contatto tamper	Si
3	Input dedicato a contatto power failure	Si
4	Contatti output	2
5	Alimentazione	12 o 24 VDC
Scheda di controllo output 16 contatti		
1	Contatti output	16
2	Input dedicato a contatto tamper	Si
3	Input dedicato a contatto power failure	Si
4	Alimentazione	12 o 24 VDC

Compatibilità

Si richiede che il materiale fornito abbia le seguenti certificazioni:

- Antintrusione: compatibile con sistema in essere presso PIT

I sistemi forniti non devono contenere componenti o dispositivi che non siano compatibili con il sistema integrato di controllo accessi e antintrusione installato presso Palazzo Italia.

È richiesto che il fornitore produca un foglio di calcolo in formato Excel in cui saranno indicati tutti i riferimenti identificativi della componente HW (es. S/N, MAC address, ecc.) e dei riferimenti di rete (elettrica, dati) a cui questa è connessa.

2.4 Realizzazione dell'impianto antintrusione Incubators IN1, IN2

La fornitura consta delle seguenti attività di dettaglio per ciascun building, la fornitura dei componenti, nella numerosità **minima, a pena di esclusione**, indicata e di seguito ulteriormente specificata, ed è da intendersi comprensiva dei servizi connessi.

Incubator 1 IN1	
Quantità	Tipologia
2	Box alimentatore supervisionato 12V8A/24V4A con batteria tampone
3	Scheda di controllo input 16 contatti
2	Scheda di controllo output 16 contatti
16	Contatto magnetico (min. grado 3 EN50131)
20	Sensore volumetrico (min. grado 3 EN50131)
1	Tastiera (min. grado 3 EN50131)
2	Sirene da interno
2	Sirene da esterno

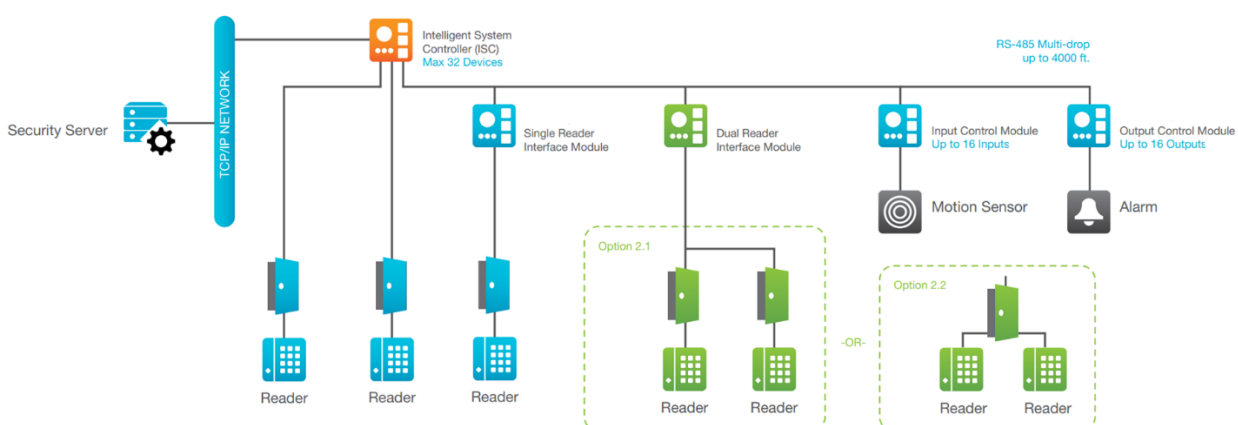
Planimetrie: Rif. Annex 1 – 1.3 Planimetria Antintrusione Incubator 1 IN1

Incubator 2 IN2	
Quantità	Tipologia
1	Box alimentatore supervisionato 12V8A/24V4A con batteria tampone
1	Scheda di controllo input 16 contatti
1	Scheda di controllo output 16 contatti
5	Contatto magnetico (min. grado 3 EN50131)
5	Sensore volumetrico (min. grado 3 EN50131)
1	Tastiera (min. grado 3 EN50131)
1	Sirene da interno
1	Sirene da esterno

Planimetrie: Rif. Annex 1 – 1.3 Planimetria Antintrusione Incubator 2 IN2

Modello di riferimento del sistema antintrusione Incubators IN1, IN2, da realizzare

Di seguito l'architettura del sistema antintrusione integrato nel sistema di controllo accessi.



L'installazione dei concentratori (box alimentazione + schede di controllo I/O) deve avvenire per quanto possibile in punti distribuiti omogeneamente a garantire la copertura dell'edificio lasciando liberi almeno 4 contatti INPUT e OUTPUT in ogni concentratore per garantire immediata scalabilità dell'impianto.

Ogni punto di concentratori deve essere costituito da un box alimentazione con batteria tampone, e un numero

sufficiente di schede di controllo input e output per coprire tutti i sensori di campo della zona sia di INPUT (es. contatti magnetici, volumetrici, ecc.) che di OUTPUT (es. sirene da interno o esterno) l'installazione deve essere effettuata per quanto possibile nei locali tecnici più prossimi alla zona e ad altezza uomo, evitando l'installazione nei controsoffitti e nei sottopavimenti. Laddove non fosse possibile effettuare l'installazione nei locali tecnici, è preferibile identificare aree coperte da videosorveglianza e non raggiungibili ad altezza uomo.

I punti di installazione delle sirene verranno concordati con la committenza in fase di progettazione esecutiva.

Il fornitore potrà proporre eventuali variazioni che riterrà migliorative (in termini di ottimizzazione dell'impianto, semplicità, ridondanza, ecc.), eventuali variazioni saranno comunque oggetto di valutazione e accettazione da parte della stazione appaltante.

Servizi connessi:

- Sopralluogo tecnico-operativo successivo all'aggiudicazione della gara, atto a definire nel dettaglio le modalità di installazione e realizzazione (a titolo esemplificativo e non esaustivo il posizionamento di elementi di campo quali concentratori e sensori, la priorità di realizzazione di porzioni di impianto rispetto ad altre);
- Fornitura e posa in opera dell'hardware, di predisposizioni elettriche e cavi;
- Licenze;
- Montaggio e cablaggio;
- Collegamento e cablaggio dei sensori in campo INPUT e OUTPUT forniti
- Collegamento e cablaggio a rete elettrica e rete dati;
- Installazione e configurazione software;
- Configurazione e settaggio di tutti i sensori antintrusione installati;
- Inserimento e configurazione mappe grafiche nel sistema integrato;
- Configurazione delle logiche antintrusione (zone, fasce orarie, ecc.)
- Collaudo e verifica delle prestazioni;
- Training per operatori;
- Redazione file DWG e documentazione tecnica as built
- Garanzia e Assistenza.

La fornitura deve inoltre comprendere eventuali altri componenti e servizi, **anche se non esplicitamente menzionati**, ma comunque necessari per la gestione, l'integrazione e il corretto funzionamento del sistema all'interno dell'infrastruttura esistente di Fondazione Human Technopole, in seguito abbreviato come FHT (ad esempio i cavi di collegamento o di alimentazione).

Si precisa che, alla data di presentazione dell'offerta nessuna delle componenti hardware della soluzione proposta deve essere stata dichiarata End-Of-Life dal costruttore, pena l'esclusione dalla procedura di gara.

La fornitura deve essere costituita **esclusivamente da materiale nuovo di fabbrica**. Sono pertanto vietati elementi (sia macro che micro, sia singoli che in gruppo, sia interni che esterni) ricondizionati, refurbished, dimostrativi, provenienti da canali di brokeraggio, da campionari, da fiere, da esposizione, da test interni o in visione presso clienti e in generale tutto ciò che non sia al primo utilizzo.

Caratteristiche Tecniche Minime Antintrusione

#	Caratteristiche Tecniche Minime	Val. min.
Scheda di controllo input 16 contatti		
1	Contatti input	16
2	Input dedicato a contatto tamper	Si
3	Input dedicato a contatto power failure	Si
4	Contatti output	2
5	Alimentazione	12 o 24 VDC
Scheda di controllo output 16 contatti		
1	Contatti output	16

2	Input dedicato a contatto tamper	Si
3	Input dedicato a contatto power failure	Si
4	Alimentazione	12 o 24 VDC
Contatto magnetico		
	Certificazione EN50131	Grado 3
	Doppio contatto per cablaggio antintrusione e controllo accessi (stato porta)	Si
Sensore volumetrico		
	Certificazione EN50131	Grado 3
	Tripla tecnologia	Si

Compatibilità

Si richiede che il materiale fornito abbia le seguenti certificazioni:

- Antintrusione: compatibile con sistema in essere presso PIT
- Sensori antintrusione: min. grado 3 EN50131

I sistemi forniti non devono contenere componenti o dispositivi che non siano compatibili con il sistema integrato di controllo accessi e antintrusione installato presso Palazzo Italia.

È richiesto che il fornitore produca un foglio di calcolo in formato Excel in cui saranno indicati tutti i riferimenti identificativi della componente HW (es. S/N, MAC address, ecc.) e dei riferimenti di rete (elettrica, dati) a cui questa è connessa.

2.5 Accessori e ricambi

La fornitura consta delle seguenti attività di dettaglio per ciascun building, la fornitura dei componenti, nella numerosità **minima, a pena di esclusione**, indicata e di seguito ulteriormente specificata, ed è da intendersi comprensiva dei servizi connessi.

Accessori e ricambi	
Quantità	Tipologia
Accessori	
1	Stampante badge dual side a colori alta risoluzione compatibile con SW di controllo accessi fornito, completa di codificatore tessere e licenze
1	Lettore/scrittore tessere MIFARE da scrivania
Ricambi	
500	Tessere MIFARE
2	Controller OSDP 32 varchi espandibile
4	Box alimentatore supervisionato 12V8A/24V4A con batteria tampone
2	Scheda di controllo varco bidirezionale
4	Lettore badge OSDP mobile enabled (tipo HID Signo 20)
2	Scheda 4 fusibili supervisionata per protezione elettroserratura
2	Scheda di controllo input 16 contatti
2	Scheda di controllo output 16 contatti
5	Contatto magnetico (min. grado 3 EN50131)
5	Sensore volumetrico (min. grado 3 EN50131)
1	Sensore rottura vetro

Servizi connessi:

- Fornitura e posa in opera degli Accessori, di predisposizioni elettriche e cavi;
- Licenze;
- Montaggio e cablaggio;
- Collegamento e cablaggio a rete elettrica e rete dati;
- Installazione e configurazione software;
- Configurazione e settaggio dei template badge per dipendenti, visitatori, fornitori, cantieri;
- Collaudo e verifica delle prestazioni;
- Training per operatori;
- Garanzia e Assistenza.

La fornitura deve inoltre comprendere eventuali altri componenti e servizi, **anche se non esplicitamente menzionati**, ma comunque necessari per la gestione, l'integrazione e il corretto funzionamento del sistema all'interno dell'infrastruttura esistente di Fondazione Human Technopole, in seguito abbreviato come FHT (ad esempio i cavi di collegamento o di alimentazione).

Si precisa che, alla data di presentazione dell'offerta nessuna delle componenti hardware della soluzione proposta deve essere stata dichiarata End-Of-Life dal costruttore, pena l'esclusione dalla procedura di gara.

La fornitura deve essere costituita **esclusivamente da materiale nuovo di fabbrica**. Sono pertanto vietati elementi (sia macro che micro, sia singoli che in gruppo, sia interni che esterni) ricondizionati, refurbished, dimostrativi, provenienti da canali di brokeraggio, da campionari, da fiere, da esposizione, da test interni o in visione presso clienti e in generale tutto ciò che non sia al primo utilizzo.

Il fornitore potrà proporre eventuali variazioni che riterrà migliorative (in termini di ottimizzazione dell'impianto, semplicità, ridondanza, ecc.), eventuali variazioni saranno comunque oggetto di valutazione e accettazione da parte della stazione appaltante.

2.6 Assistenza

Il servizio di Assistenza si intende attivo dalla chiusura con esito positivo del collaudo a valle della fornitura e realizzazione delle opere di cui sopra.

Il servizio di Assistenza comprende:

- Rinnovo biennale pacchetto licenze;
- Canone di assistenza per n. 2 anni;
- Quota dedicata a servizi extra canone (intervento on-site presso sede HT di un tecnico per una giornata di 8 ore con spese di trasferta incluse) e ricambi originali (con % minima di sconto su listino ufficiale LENEL in vigore al momento della quotazione).

Canone Servizio di Assistenza

Fatte salve le garanzie contrattuali, il canone del servizio di assistenza prevede:

- Intervento di controllo preventivo su base annuale. Minimo n.1 intervento/anno.
- Interventi di assistenza da remoto. Minimo n. 300 interventi/anno.
- Interventi di assistenza on-site comprensivo di minimo n. 6 interventi/anno ai fini di manutenzione preventiva, correttiva, evolutiva e revamping obsolescenze (l'intervento on-site presso sede HT di un tecnico per una giornata di 8 ore con spese di trasferta incluse).
- Canali di contatto per richiesta di assistenza attivi H24.
- Rapporto di fine intervento con dettaglio delle attività eseguite.
- Eventuale adeguamento della documentazione in caso di modifiche all'impianto.

La manutenzione preventiva deve prevedere controlli atti a verificare la piena funzionalità di: Applicativo, Server, Postazioni PC Client, pannelli di controllo, alimentatori, batterie, lettori badge, attuatori, sensori e pulsanti (ove presenti), comunicazione tra le componenti del sistema; oltre che a verificare la presenza di eventuali anomalie sugli elementi del sistema.

L'attività di manutenzione preventiva annuale dovrà essere eseguita in riferimento alle normative vigenti.

Controlli minimi previsti nell'intervento annuale:

- Verifica Server e PC Client con software di gestione;
- Verifica ora e data presente;
- Verifica comunicazione con tutti i pannelli presenti nell'impianto;
- Verifica presenza di eventuali segnalazioni di errore/anomalia;
- Verifica funzionamento del sistema di backup;
- Verifica integrità archivi;
- Verifica alimentatori e condizione di carica delle batterie;
- Verifica orario e segnalazioni interne pannello;
- Verifica corretto funzionamento on line e stand alone;
- Verifica livello di pulizia lettori e banda magnetica e/o di prossimità;
- Verifica corretta lettura tessere;
- Verifica corretto funzionamento dei sensori antintrusione
- Verifica sblocco varco da pulsante se presente;
- Verifica lettura stato porta;
- Verifica corretta attuazione elettromagnete, incontro elettrico o elettroserratura.

Tempi di intervento minimi:

Manutenzione preventiva (1/y): schedato preventivamente sulla base delle esigenze HT, secondo calendario di intervento se di durata superiore a un giorno.

Assistenza remota: entro 1 ora dalla chiamata

Assistenza onsite: blocco totale del sistema (entro 4 ore), blocco di un edificio o blocco di un varco critico (entro 8 ore), blocco di un varco non critico o guasto non bloccante (NBD o concordato in data successiva se espressamente richiesto da HT)

Il servizio di assistenza sul sistema prevede l'accesso ai dati personali in esso contenuti, pertanto l'attivazione del servizio deve essere subordinata all'adempimento dei requisiti (e alle relative nomine) previsti dalla normativa vigente.

3 REQUISITI

I seguenti requisiti si riferiscono a tutte le attività oggetto dell'appalto.

3.1 Requisiti tecnico-professionali

Il fornitore dovrà già essere preventivamente qualificato come rivenditore autorizzato (VAR) dal produttore del sistema in essere presso PIT.

Al fine di garantire adeguata solidità e affidabilità dell'erogazione dei servizi oggetto di appalto, il fornitore dovrà avere almeno una sede operativa in Lombardia e avere in organico:

- min. 5 tecnici certificati alla realizzazione impianti secondo normative CEI 79/3 e EN 50131
- min. 3 tecnici certificati ad operare dal produttore del sistema in essere presso PIT di livello almeno Professional Access o Intrusion
- min. 1 tecnico certificato ad operare dal produttore del sistema in essere presso PIT di livello almeno Expert Access e Intrusion

Si rende necessario allegare la documentazione attestante i requisiti, tra cui curriculum vitae e riferimenti delle certificazioni in corso di validità.

3.2 Requisiti ICT

Sicurezza dell'architettura

Deve essere presente un'architettura affidabile (es: i software usati sono di mercato, supportati dai produttori, inoltre vengono seguiti i canoni del CIS o del NIST per l'hardening delle componenti): tutte le componenti software che la costituiscono la piattaforma per fornire il servizio, devono essere mantenute ed aggiornate regolarmente.

Conformità agli standard

Deve essere garantita la conformità al GDPR.

Gestione delle vulnerabilità

Le vulnerabilità vengono trattate non appena vengono identificate dal fornitore, dal produttore o da terzi: le CVE – Common Vulnerability Exposure sono notificate attraverso vari canali noti, in primis quelli dei vendor specifici di ogni componente software, il trattamento di tali vulnerabilità deve essere in linea con un processo di gestione delle vulnerabilità (processi di Vulnerability Management oppure Patch-Management) il quale miri a trattare le vulnerabilità di livello critico, classificate come tali dal CVSS (Common vulnerability Scoring System) Scoring versione 3.1 o superiore, entro 30 giorni solari dalla pubblicazione della CVE.

Risposta agli incidenti

Deve essere garantito uno SLA appropriato (entro 24 ore dall'ingaggio) per gestire gli incidenti di sicurezza ICT in modo tempestivo, senza nessun costo aggiuntivo a carico della Fondazione.

Crittografia

- Deve essere garantita la crittografia dei dati in transito (ad esempio: HTTPS su TLS 1.2).
- La crittografia dei dati "at rest" deve essere possibile
- Le credenziali dell'account, le secret devono essere crittografati e non possono essere memorizzati in chiaro.

Controllo dell'accesso dell'utente

L'autenticazione per l'accesso alla piattaforma deve avvenire in modo centralizzato integrando:

- tramite LDAP se il sistema è on premise
- tramite Single Sign on utilizzando SAML2 con EntraID, SP-initiated, se il sistema è basato su cloud.

Hardening

Il sistema deve essere ben protetto, e deve consentire, ad esempio:

- AD Joined se si tratta di una macchina Windows
- MS Defender in modalità EDR deve poter essere installato.
- non dovrebbe essere richiesto un amministratore locale per avere il servizio, invece FHT ICT potrebbe impostare il grantset corretto per rendere l'account in grado di raggiungere le sue funzionalità, se il fornitore fornisce le informazioni appropriate per farlo.

Registri di audit

Tutte le azioni degli utenti devono essere tracciate e registrate.

Resilienza

Il fornitore della piattaforma dovrebbe fornire informazioni utili per realizzare un backup affidabile, quali:

- file e directory, chiavi di registro da sottoporre a backup
- eventuali accorgimenti per il backup degli elementi di cui sopra
- come determinare il backup è avvenuto con successo
- una procedura per il ripristino del servizio partendo da un backup avvenuto con successo

Monitoraggio

Il fornitore deve fornire informazioni utili per integrare la piattaforma nel sistema di monitoraggio già presente.

Supporto/Maintenance

Il dipartimento ICT della Fondazione si farà carico del solo sistema operativo della Virtual Machine e della infrastruttura ICT sottostante, il fornitore si farà carico di tutto ciò che è necessario per fare funzionare in modo corretto l'applicativo oggetto di fornitura.

4. ALTRI SERVIZI

4.1. COLLAUDO

Il collaudo si svolgerà mediante le seguenti attività minime:

- verifica della consegna di tutti i componenti offerti
- test di accensione/spengimento e attivazione/disattivazione degli impianti installati e integrati
- test di funzionamento dei varchi controllati
- test di funzionamento delle aree protette da antintrusione
- test di funzionamento con casi d'uso che interessano l'integrazione degli impianti
- test di funzionamento dell'integrazione dati presenze mediante file per interfaccia con software di gestione paghe Zucchetti HR Workflow (tramite agent dedicato): generazione, invio e backup
- verifica delle configurazioni effettuate e corrispondenza con la documentazione prodotta
- valutazione della completezza ed esaustività della documentazione prodotta (a titolo esemplificativo file DW, documentazione tecnica as built, file configurazioni, ecc.)

L'attività si svolgerà alla presenza e in contraddittorio col fornitore presso i locali della stazione appaltante. Eventuali non conformità dovranno essere risolte entro 7 giorni solari dal collaudo. L'attività terminerà con la sottoscrizione del verbale di collaudo in contraddittorio con il fornitore.

La data di consegna del verbale di collaudo verrà considerata quale data di accettazione fornitura e avvio del servizio di assistenza.

4.2. GARANZIA

Il fornitore, in collaborazione con il costruttore degli apparati, deve prevedere e offrire, **per un periodo pari a quello indicato dai requisiti minimi di legge** un servizio di garanzia che assicuri il mantenimento nel tempo degli apparati in uno stato di funzionamento idoneo allo svolgimento delle funzioni a cui sono preposti.

All'interno dell'offerta il fornitore dovrà illustrare le modalità di erogazione del servizio di garanzia, che ha per oggetto tutti gli oggetti descritti e specificati nel presente capitolato Tecnico.

Per ciascun apparato dovrà essere sempre possibile stipulare contratti aggiuntivi di assistenza o di estensione della garanzia in Italia con le stesse caratteristiche del servizio di manutenzione minimo richiesto.

Nel Piano di realizzazione, così come descritto al paragrafo 5.2., dovranno essere indicati tutti i punti di contatto col servizio di supporto in particolare per quanto riguarda numero di telefono in Italia e indirizzo e-mail. Il fornitore è altresì tenuto ad indicare l'organizzazione aziendale secondo il quale il servizio di supporto opera e il workflow operativo che seguono le richieste di assistenza.

Il servizio di sostituzione in loco dei componenti guasti e/o mal funzionanti è a carico del fornitore.

Questo servizio prevede l'intervento in loco presso il sito ove sono installati gli apparati oggetto della fornitura di almeno un tecnico specializzato nella tecnologia di questi ultimi. Le operazioni incluse nel servizio sono la fornitura, consegna e installazione di eventuali parti di ricambio in sostituzione di quelle difettose o guaste.

Il fornitore inoltre dovrà poter consentire alla Fondazione Human Technopole, in maniera diretta e attraverso il costruttore degli apparati, il download del firmware e del software di gestione degli apparati, delle relative patch e della opportuna documentazione.

5. MODALITA' DI ESECUZIONE DELL'APPALTO

5.1. Modalità di fornitura e installazione

Il servizio di consegna ed installazione dovrà essere erogato dal fornitore, attraverso personale specializzato, presso i locali della Fondazione Human Technopole. Tutte le attività si intendono **comprehensive di ogni onere relativo al trasporto, facchinaggio, consegna ai piani, posa in opera, asporto dell'imballaggio e di qualsiasi altra attività ad esse strumentale**. Il fornitore, inoltre, dovrà dotarsi di mezzi opportuni e/o di quanto altro necessario a trasportare, scaricare e a collocare la fornitura nei locali.

Il fornitore garantirà, durante tutte le fasi di lavorazione, il rispetto delle normative vigenti in materia di tutela della salute e della sicurezza nei luoghi di lavoro.

5.2. Piano di realizzazione

Nei 30 gg solari successivi alla stipula contrattuale il fornitore deve presentare il Piano di realizzazione della fornitura conforme nei tempi e modi a quanto stabilito nel presente capitolato.

Il fornitore dovrà fornire tutti gli elementi utili per valutare nel suo complesso il processo di consegna, installazione e il collaudo che metterà in atto per consegnare nei termini richiesti la fornitura offerta, pertanto dovranno essere indicate le attività realizzative previste e i relativi tempi di attuazione.

Nel piano di realizzazione le attività devono garantire la continuità di invio dei transiti allo studio paghe per elaborazione dati presenze.

È richiesto che vengano dettagliate:

- il work flow aziendale che descriva come sarà strutturato il processo di consegna e installazione nelle sue varie fasi (es. attività propedeutiche, realizzazione, consegna, installazione e collaudo);
- le strategie che verranno adottate per rispettare i termini di consegna del presente capitolato e recuperare i possibili ritardi dovuti a imprevisti;
- **descrizione della realizzazione delle opere in campo e relative interferenze con altre lavorazioni negli spazi**, è necessario concordare le attività col committente;
- la descrizione delle procedure di collaudo così come descritte nel paragrafo dedicato.

Durante tutta la fase esecutiva di consegna, installazione e collaudo della fornitura, verrà condotto un monitoraggio costante dello stato di avanzamento dell'attività, allo scopo di verificare che il fornitore rispetti le varie scadenze temporali e le modalità di consegna, installazione e collaudo definite nel presente capitolato.

Il fornitore, all'atto della consegna delle apparecchiature, dovrà fornire tutti i manuali in italiano e/o inglese delle apparecchiature fornite in formato elettronico, dovrà fornire anche un inventario, sia cartaceo che elettronico (con: tipo/modello/seriale/configurazione/consumi elettrici) della fornitura. Dovrà altresì consegnare tutti gli eventuali accessori previsti e non installati.

Il fornitore dovrà indicare all'interno del Piano di realizzazione:

- il gruppo di lavoro con il numero e la tipologia del personale staffato
- un punto di contatto unico, nominativi delle persone di riferimento compresi, per le questioni amministrative;
- un punto di contatto unico, nominativi delle persone di riferimento compresi, per le problematiche e l'organizzazione del sopralluogo ispettivo;
- un punto di contatto unico, nominativi delle persone di riferimento compresi, per le problematiche di consegna e installazione;
- un punto di contatto unico, nominativi delle persone di riferimento compresi, per le problematiche tecniche.

5.3. Sopralluogo ispettivo

Il fornitore affidatario **dovrà** effettuare un sopralluogo ispettivo al fine di valutare in autonomia le infrastrutture offerte dai locali interessati nell'intervento. Esso potrà essere svolto prima della consegna del Piano di Realizzazione, prendendo contatto con la stazione appaltante in modo da fissare la data del sopralluogo con almeno 2 gg lavorativi di anticipo rispetto alla data desiderata.

In particolare, il fornitore dovrà:

1. Eseguire un sopralluogo durante il quale dovranno essere raccolte tutte le informazioni propedeutiche alla consegna e installazione presso la sede. La necessità di dovere eseguire ulteriori sopralluoghi dovrà essere debitamente motivata dal fornitore.
2. Inviare entro 2 giorni lavorativi dallo svolgimento il verbale di sopralluogo con tutte le informazioni rilevanti:
 - a. scopo del sopralluogo;
 - b. dettagli della sede;
 - c. nome, cognome, recapito telefonico del personale del fornitore;
 - d. nome, cognome, recapito telefonico del personale della Fondazione che ha seguito il sopralluogo;
 - e. esito del sopralluogo: in caso di esito negativo dovranno essere evidenziate tutte le criticità emerse e proposte le eventuali azioni correttive;
 - f. firma per accettazione del personale della sede che ha seguito il sopralluogo;
 - g. al verbale di sopralluogo potrà essere allegata eventuale documentazione rilevante (es: documentazione fotografica, ecc.).

Obiettivo dei sopralluoghi sarà l'ottimizzazione della logistica inerente alla consegna, installazione e collaudo delle apparecchiature oggetto della fornitura e valutazione di tutte le possibili interferenze in osservanza alle vigenti leggi sulla sicurezza dei luoghi di lavoro.

6. TEMPISTICHE DI ESECUZIONE DELL'APPALTO

È prevista la consegna e il collaudo della fornitura nella sua interezza.

6.1. Modalità di consegna

È richiesto che detta procedura di consegna sia strutturata nelle seguenti fasi:

- A) **Sopralluogo ispettivo:** da effettuarsi, secondo le specifiche indicate nel paragrafo dedicato, necessariamente prima della consegna del Piano di realizzazione;
- A) **Presentazione Piano di realizzazione:** entro 30 gg solari a partire dalla data di sottoscrizione o del verbale di avvio ove precedente;
- B) **Consegna e installazione della fornitura:** entro 110 gg solari a partire dalla data di sottoscrizione o del verbale di avvio ove precedente;
- C) **Collaudo della fornitura:** le specifiche relative al collaudo sono dettagliate nella sezione dedicata. Nel caso di esito positivo del collaudo, la data del verbale di collaudo verrà considerata quale data di accettazione fornitura da cui decorre il periodo di assistenza;

il termine massimo di consegna, installazione e collaudo è stabilito in massimo 150 giorni solari.

Il Fornitore si impegna espressamente alla consegna, installazione e collaudo di tutti gli apparati offerti nei tempi prestabiliti: il mancato rispetto da parte del Fornitore delle suddette tempistiche, comporta l'applicazione delle previste penali.

7. TRATTAMENTO E TUTELA DEI DATI PERSONALI

L'aggiudicatario dichiara di aver ricevuto prima della sottoscrizione del contratto di fornitura/servizio le informazioni di cui agli artt. 13 e 14 del regolamento UE n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (nel seguito anche "Regolamento UE"), circa il trattamento dei dati personali, conferiti per la sottoscrizione e l'esecuzione del contratto stesso e di essere a conoscenza dei diritti riconosciuti ai sensi della predetta normativa.

Con la sottoscrizione del contratto, il rappresentante legale del fornitore acconsente espressamente al trattamento dei dati personali come sopra definito, si impegna ad adempiere agli obblighi di rilascio dell'informativa e di richiesta del consenso, ove necessario, nei confronti delle persone fisiche interessate di cui sono forniti dati personali nell'ambito dell'esecuzione del contratto per le finalità descritte nel disciplinare di gara e sopra richiamate.

La S.A. acconsente espressamente al trattamento da parte dell'aggiudicatario dei dati relativi alla fatturazione, rendicontazione e monitoraggio per le finalità connesse all'esecuzione del contratto.

Inoltre, in adempimento agli obblighi di legge che impongono la trasparenza amministrativa (art. 32 L. 190/2012, art. 29 D. Lgs. 50/2016 e s.m.i.), il fornitore prende atto della pubblicazione e diffusione dei dati e/o della documentazione che la legge impone di pubblicare, tramite il sito internet <https://humantechnopole.it/> sezione Amministrazione trasparente.

Con la sottoscrizione del contratto il fornitore acconsente espressamente al trattamento dei dati personali e si impegna a improntare il trattamento dei dati ai principi di correttezza, liceità e trasparenza nel pieno rispetto della normativa vigente (Regolamento UE 2016/679), ivi inclusi gli ulteriori provvedimenti, comunicati ufficiali, autorizzazioni generali, pronunce in genere emessi dall'Autorità Garante per la protezione dei dati personali. In particolare, si impegna ad eseguire i soli trattamenti funzionali, necessari e pertinenti all'esecuzione delle prestazioni contrattuali e, in ogni modo, non compatibili con le finalità per cui i dati sono stati raccolti.

L'aggiudicatario si impegna ad adottare le misure di sicurezza di natura fisica, logica, tecnico ed organizzativa adeguate a garantire un livello di sicurezza adeguato al rischio, ivi compresa quelle specificate nel contratto, unitamente ai suoi allegati; si impegna, altresì ad osservare le vigenti disposizioni in materia di sicurezza e privacy e a farle osservare ai relativi dipendenti e collaboratori, opportunamente autorizzati al trattamento dei Dati personali.

L'aggiudicatario prende atto che HT potrà operare verifiche periodiche, ispezioni ed audit, anche tramite soggetti terzi autorizzati dalla stessa, volti a riscontrare l'applicazione e l'adeguatezza delle misure di sicurezza dei dati personali applicate.

Qualora per l'esecuzione della fornitura o del servizio sia necessario il trattamento, da parte del Fornitore, di dati personali di una o più categorie di interessati gestiti dalla Fondazione HT, quest'ultima, nella sua qualità di titolare del trattamento di tali dati personali, designa il Fornitore, ai sensi dell'art. 28 del Regolamento con apposito atto di nomina, responsabile esterno del trattamento di dati personali effettuato per conto del titolare nella esecuzione del presente contratto. A tal fine, il Fornitore si impegna ad improntare il trattamento dei dati ai principi di correttezza, liceità e trasparenza nel pieno rispetto di quanto disposto dall'art. 5 del Regolamento UE e nei provvedimenti, comunicati ufficiali, autorizzazioni generali, pronunce in genere emessi dall'Autorità Garante per la Protezione dei Dati Personali, limitandosi ad eseguire i soli trattamenti funzionali, necessari e pertinenti all'esecuzione delle prestazioni contrattuali e, in ogni modo, non incompatibili con le finalità per cui i dati sono stati raccolti.

Il Fornitore si impegna all'adozione delle misure tecniche e organizzative così come individuate nel contratto.