

CONTRATTO PER L’AFFIDAMENTO DEL SERVIZIO DI
CONSULENZA PER IL RAGGIUNGIMENTO DELLE MISURE MINIME DI
SICUREZZA

(D.Lgs 82/2005, circolare AGID n. 2 del 18/04/2017, Nota MIUR n. 3015 del 20/12/2017)

CIG. Z3222 B57B8

tra

Istituto Comprensivo Statale “G. Leopardi” di seguito denominata “Scuola” con sede a Torre Annunziata, alla via Cavour Cod. Fisc.90082020638, nella persona del Dirigente Scolastico Prof. Antonella d’Urzo, in prosieguo anche denominata più semplicemente “Committente”

e

La società **INFOSYS TEAM S.r.l.** con sede in Marigliano, Corso Umberto n°188 P.IVA e C.F. 06268691216 nella persona di Salvatore GUILLARI in prosieguo anche denominata più semplicemente “Affidatario”.

premesse

- ❖ che l’Affidatario ha dimostrato, nella persona del sig. Salvatore GUILLARI (C.F. GLL SVT 67R05 F839M), che viene, di fatto, nominato “Consulente della sicurezza informatica”, il possesso dei requisiti dichiarati in sede di offerta
- ❖ che il sig. Salvatore GUILLARI è persona conosciuta dal Committente e ritenuta degna di fiducia, in quanto, da anni, impegnata nel settore tecnico/informatico;
- ❖ che la società INFOSYS Team S.r.l., e lo stesso sig. GUILLARI, hanno, a più riprese e nel corso degli anni, lavorato per questa scuola con piena soddisfazione del Committente e l’esecuzione dei lavori è sempre stata “a regola d’arte”, senza ritardi nelle consegne e tempestivi negli interventi di manutenzione alle attrezzature nella dotazione della Scuola;
- ❖ che sono state positivamente espletate le verifiche antimafia secondo la normativa vigente;
- ❖ che, conseguentemente, può procedersi alla stipula del contratto.

Tutto ciò premesso, fra le parti come sopra costituite e rappresentate, si conviene e stipula quanto segue.

ARTICOLO 1

Valore giuridico delle premesse e degli allegati

1. Le premesse, gli allegati e tutti i documenti richiamati nel presente contratto ne costituiscono parte integrante e sostanziale ed hanno ad ogni effetto valore di patto.

ARTICOLO 2

Oggetto del Contratto

1. Il Committente affida con il presente contratto all’Affidatario, che accetta, la realizzazione del “Servizio di Consulente della sicurezza informatica”

L’Affidamento oggetto del presente contratto si specifica nelle seguenti attività e fa riferimento alla Circolare AgID del 17 marzo 2017 n. 1/2017 contenente le “Misure minime di sicurezza ICT per le

pubbliche amministrazioni” successivamente sostituita dalla circolare n. 2/2017 del 18 aprile 2017 per correggere alcuni errori di carattere formale:

- Implementare un inventario delle risorse attive
- Aggiornare l’inventario quando nuovi dispositivi approvati vengono collegati in rete.
- Gestire l’inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l’indirizzo IP.
- Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l’installazione di software non compreso nell’elenco.
- Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.
- Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.
- Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall’organizzazione.
- Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.
- Le immagini d’installazione devono essere memorizzate offline.
- 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).
- Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.
- Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.
- Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.
- Assicurare l’aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.
- Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.
- 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.).
- Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.
- Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.
- Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.
- Mantenere l’inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.
- Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell’amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.
- Quando l’autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).
- Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging)
- Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).
- Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.
- Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.
- Le utenze amministrative anonime, quali “root” di UNIX o “Administrator” di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l’immutabilità di chi ne fa uso.
- Conservare le credenziali amministrative in modo da garantire disponibilità e riservatezza.
- Se per l’autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.
- 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 sono mantenuti aggiornati in modo automatico.
- Installare su tutti i dispositivi firewall ed IPS personali.
- Limitare l’uso di dispositivi esterni a quelli necessari per le attività aziendali.
- Disattivare l’esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.
- Disattivare l’esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.
- Disattivare l’apertura automatica dei messaggi di posta elettronica.
- Disattivare l’anteprima automatica dei contenuti dei file.
- Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.
- Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l’impiego di strumenti antispam.
- Filtrare il contenuto del traffico web.
- 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).

- Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.
- Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.
- 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.
- Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica
- Bloccare il traffico da e verso url presenti in una blacklist.

ARTICOLO 3

Disciplina contrattuale del rapporto

1. Il rapporto è regolato dalle disposizioni contenute nei seguenti documenti, che si applicheranno, in casi di discordanza, nell'ordine qui appresso indicato:
 - l'offerta tecnica e l'offerta economica presentate dall'Affidatario in sede di preventivo
 - le norme e i documenti richiamati nel presente contratto d'appalto e nei documenti sopra menzionati.
2. I predetti documenti ed elaborati fanno parte integrante del presente contratto, anche se non materialmente allegati, e l'Affidatario, sig. Salvatore GUILLARI, dichiara espressamente di ben conoscerli e di accettarli in ogni loro parte.

ARTICOLO 4

Esatta conoscenza del servizio da eseguire

1. L'Affidatario dichiara espressamente di aver esaminato con la massima cura e attenzione gli atti, i provvedimenti, le circolari e i documenti richiamati, e di essersi reso conto esattamente del servizio da eseguire, delle sue particolarità, nonché di tutte le circostanze generali e particolari che possono influire sull'esecuzione del medesimo.

ARTICOLO 5

Luogo di esecuzione del contratto

1. Le prestazioni oggetto del presente contratto dovranno essere eseguite prettamente presso la sede del Committente.

Variazioni del servizio

1. È in facoltà del Committente introdurre nel suo esclusivo interesse, in fase di esecuzione del servizio, le ulteriori specificazioni o modificazioni non sostanziali che riterrà opportune ai fini della buona riuscita e della funzionalità della prestazione inerente il servizio, senza che l'Affidatario possa, per ciò solo, far valere pretese di alcun genere in ordine a maggiori compensi o indennizzi di sorta, nonché in ordine a richieste di maggior tempo per il completamento delle prestazioni oggetto del contratto.
2. L'Affidatario non potrà, invece, apportare al servizio variazioni o aggiunte, salvo che le stesse siano state preventivamente indicate, richieste o autorizzate dal Committente.

ARTICOLO 6

Corrispettivo dell'appalto

1. Il corrispettivo dell'appalto è così stabilito:
euro 1.000,00 (mille/00) al netto d'IVA, corrispondente all'importo offerto in sede di offerta dall'Affidatario quale prezzo forfettario ed onnicomprensivo del servizio richiesto con riferimento a tutte le attività previste nel presente contratto,
2. Il corrispettivo è fisso e invariabile, e come tale si intende comprensivo di ogni onere o spesa occorrente per l'esecuzione del servizio a perfetta regola d'arte.
3. Non si procederà alla revisione prezzi, né troverà applicazione al presente contratto l'art. 1664, primo comma, del codice civile.

ARTICOLO 7

Modalità di pagamento

1. Il Committente corrisponderà all'Affidatario l'importo di cui all'articolo precedente secondo le seguenti specifiche modalità:
 - l'erogazione del 50% del predetto importo, previa presentazione della relativa fattura per l'importo totale (€ 1.000,00 oltre IVA al 22%), entro 60 giorni dalla presentazione della stessa.
 - l'erogazione del rimanente 50%, entro i 60 giorni successivi alla prima scadenza.
2. Il pagamento di tutti gli importi di cui al precedente comma è subordinato al rilascio da parte dell'Affidatario delle certificazioni atte a comprovare il regolare versamento dei contributi in favore dei dipendenti (modello DURC).
3. I predetti importi verranno corrisposti dal Committente a mezzo bonifico bancario sul conto corrente n. 6800 intestato a INFOSYS Team S.r.l. presso il Banco di Napoli Ag. di Marigliano codice IBAN: **IT57 E010 1039 9621 00000006 800**

ARTICOLO 8

Tempi di esecuzione

1. Il Servizio indicato al precedente art. 2 ha la durata di 1 (uno) anno deve essere avviato a partire dal giorno successivo alla stipula del presente contratto tra il Committente e l'Affidatario. Il Committente si riserva in ogni caso di chiedere in caso di urgenza l'immediato avvio delle attività prima della stipula del contratto.
2. Il Servizio oggetto del presente contratto si conclude allo scadere del 364° giorno decorrente dalla data di stipula del contratto.

ARTICOLO 9

Collaudo - Verifica e controllo sull'attività

1. Il Committente potrà effettuare uno o più verifiche per ogni attività di sviluppo informatico svolte nell'ambito del Servizio.
2. Le verifiche delle predette attività sono eseguiti da un gruppo di collaudo nominato dal Committente.
3. A seguito di ciascuna verifica verrà redatto apposito verbale, congiuntamente sottoscritto dal gruppo di collaudo, per il Committente da un proprio funzionario a ciò delegato, e dall'Affidatario, nel quale siano almeno indicate le seguenti informazioni:

- l'oggetto della verifica;
- la tipologia di verifica (provvisoria o definitiva);
- la data di inizio e di conclusione delle operazioni di verifica;
- il contesto operativo in cui è stata effettuata la verifica;
- i prodotti, i servizi e le prestazioni esaminate;
- le procedure seguite per l'esecuzione della verifica;
- i risultati ottenuti;
- l'esito della verifica.

4. Nella fase di esecuzione del contratto il Committente si riserva la più ampia facoltà di verificare in ogni momento e anche senza preavviso che l'esecuzione del servizio avvenga in conformità alle specifiche richieste ed alle previsioni contrattuali.

5. Il Committente può effettuare le suddette verifiche sia a mezzo di proprio personale, sia con personale esterno all'uopo delegato.

6. L'esito favorevole delle verifiche non esonera l'Affidatario dai propri obblighi e dalle responsabilità; pertanto, qualora, anche successivamente all'effettuazione delle verifiche stesse, venga accertata la non corrispondenza delle modalità di esecuzione del servizio alle prescrizioni contrattuali, l'Affidatario deve provvedere a sua cura e spese al tempestivo adempimento di tutte le prescrizioni ordinate dal Committente al fine di ricondurre l'attività alle suddette prescrizioni di contratto.

7. Fermo quanto sopra, qualora durante lo svolgimento del servizio il Committente accertasse che lo stesso non risulti eseguito a perfetta regola d'arte o in difformità rispetto alle norme ed alle specifiche indicate nel contratto, lo stesso provvederà ad intimare all'Affidatario di adempiere a quanto necessario entro un termine determinato.

8. Qualora l'Affidatario non ottemperi a quanto ordinato nel termine fissato, il Committente può dichiarare la risoluzione di diritto del presente contratto.

ARTICOLO 10

Divieto di cessione del contratto - Cessione del credito - Subappalto

1. È fatto assoluto divieto all'Affidatario di cedere ad altri, l'esecuzione di tutto o di parte del servizio. La violazione di tale divieto comporta la risoluzione di diritto del contratto.
2. L'Affidatario può cedere a terzi i crediti derivanti alla stessa dal presente contratto, ma tale cessione è subordinata all'accettazione espressa da parte del Committente. È fatto, altresì, divieto all'Affidatario di conferire, in qualsiasi forma, procure all'incasso.
3. L'Affidatario può ricorrere al subappalto limitatamente previa autorizzazione scritta del Committente.

ARTICOLO 11

Riservatezza

1. L'Affidatario, in ottemperanza a quanto previsto dal D.Lgs. n. 196/2003 e in quanto Responsabile del trattamento dei dati gestiti nell'ambito delle prestazioni oggetto del presente contratto, assume l'obbligo di mantenere riservati tutti i dati e le informazioni di cui venga in possesso nell'espletamento del servizio, di non divulgarli e di non farne oggetto di sfruttamento e si impegna, altresì, a garantire il medesimo impegno da parte di tutti i soggetti dei quali si avvalga, a qualsiasi titolo, per l'espletamento delle prestazioni contrattuali. In particolare si precisa che tutti gli obblighi in materia di riservatezza devono essere rispettati per i due anni successivi alla cessazione di efficacia del rapporto contrattuale.
2. È in facoltà del Committente verificare il rispetto dell'obbligo di riservatezza di cui al presente articolo. Il mancato adempimento di tale obbligo rappresenta colpa grave e sarà considerato motivo per la risoluzione del contratto da parte del Committente.

ARTICOLO 12

Risoluzione del contratto

1. È in facoltà del Committente di dichiarare la risoluzione di diritto del presente contratto, ai sensi dell'art. 1456 del codice civile:
- a) qualora per grave inadempimento oppure per inosservanza degli obblighi e delle condizioni stabilite nei documenti contrattuali, l'Affidatario comprometta l'esecuzione a regola d'arte del servizio;
 - b) nell'ipotesi prevista dal precedente art. 13 di ingiustificata sospensione del servizio protratta per oltre 15 giorni;
 - c) qualora l'Affidatario non ottemperi a quanto ordinato nel termine fissato di cui al precedente art. 14;
 - e) quando risulti accertato il mancato rispetto della disciplina regolante la cessione del contratto ed il subappalto;
 - f) in caso di liquidazione dell'Affidatario, di cessazione di attività, di amministrazione straordinaria, oppure nel caso fallimento o altra procedura concorsuale ad esso equiparata;
 - g) nel caso in cui venga meno la certificazione EN ISO 9001:2000 rilasciata all'Affidatario o, se del caso, ad una delle società costituenti il raggruppamento temporaneo di imprese o alla società subappaltatrice nel caso di subappalto, per un periodo superiore ai sei mesi;
 - h) in caso di esito negativo del controllo di veridicità delle dichiarazioni rese dall'Affidatario in sede di gara ai sensi degli articoli 46 e 47 del D.P.R. 445/2000, fatto salvo quanto previsto dall'art. 71, comma 3 del D.P.R. 445/2000.

ARTICOLO 13

Controversie

1. Qualsiasi controversia o contestazione comunque relativa all'esecuzione del servizio non consentirà all'Affidatario di sospendere la prestazione, né di rifiutarsi di eseguire le disposizioni ricevute.
2. Per le eventuali controversie che non potessero essere preventivamente composte in via bonaria, le parti dichiarano di indicare in via esclusiva quale Foro competente quello di Napoli.

ARTICOLO 14

Consenso al trattamento dei dati

1. Le parti dichiarano di essersi reciprocamente comunicate oralmente e prima della sottoscrizione del presente contratto le informazioni di cui all'articolo 13 del D.Lgs. n. 196/2003 recante "Codice in materia di protezione dei dati personali" circa il trattamento dei dati personali conferiti per l'esecuzione del contratto stesso e di essere a conoscenza dei diritti che spettano loro in virtù dell'art. 7 della citata normativa.
2. Il Committente tratta i dati ad essa forniti per la gestione del contratto e l'esecuzione economica ed amministrativa dello stesso e per l'adempimento degli obblighi legali ad esso connessi.
3. Le parti si impegnano ad improntare il trattamento dei dati ai principi di correttezza, liceità e trasparenza nel pieno rispetto di quanto definito dal citato D.Lgs. n. 196/2003, con particolare attenzione a quanto prescritto con riguardo alle misure minime di sicurezza da adottare.

Il Committente

L'Affidatario