

CAPITOLATO SPECIALE D'APPALTO

G005_2026 - Procedura telematica aperta ex art. 71 D.lgs. 36/2023 per l'affidamento di un servizio Security Operations Center (SOC) in modalità “as a Service” con il criterio dell’offerta economicamente più vantaggiosa sulla base del miglior rapporto qualità/prezzo - CPV 72500000-0 Servizi informatici - CUI S01279680480202600001

1. Premesse

1.1 Contesto di riferimento e obiettivi

L'Università degli Studi di Firenze (di seguito UNIFI), in linea con gli obblighi previsti dalla Direttiva NIS 2 (Direttiva UE 2022/2555) e dal contesto normativo italiano in materia di sicurezza delle reti e dei sistemi informativi, intende rafforzare la propria capacità di prevenzione, rilevamento e risposta agli incidenti di sicurezza informatica.

La crescente complessità delle minacce cyber e l'esigenza di garantire la continuità operativa dei servizi digitali dell'Ateneo rendono necessaria l'adozione di un servizio SOC, Security Operations Center fornito in modalità “as a Service” (SOCaaS), ovvero un servizio gestito di monitoraggio, analisi e risposta agli eventi di sicurezza operativo 24 ore su 24, 7 giorni su 7.

Il presente Capitolato definisce i requisiti minimi obbligatori, i criteri di valutazione e le modalità per l'affidamento del servizio SOCaaS, nell'ottica di individuare la soluzione economicamente più vantaggiosa per l'Ateneo.

1.2 Riferimenti normativi

L'offerta tecnica dovrà essere conforme e ispirarsi ai seguenti riferimenti:

- Decreto Legislativo 36/2023 (Codice dei Contratti Pubblici) e s.m.i.
- Regolamento (UE) 2016/679 (GDPR).
- Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni (AgID).

- Direttiva NIS2 (UE) 2022/2555 recepita con D.Lgs. 138/2024
- Determinazioni ACN come da DL 138/2024
- Framework Nazionale per la Cybersecurity e la Sicurezza Informatica (ACN).
- Standard internazionali della famiglia ISO/IEC 27000

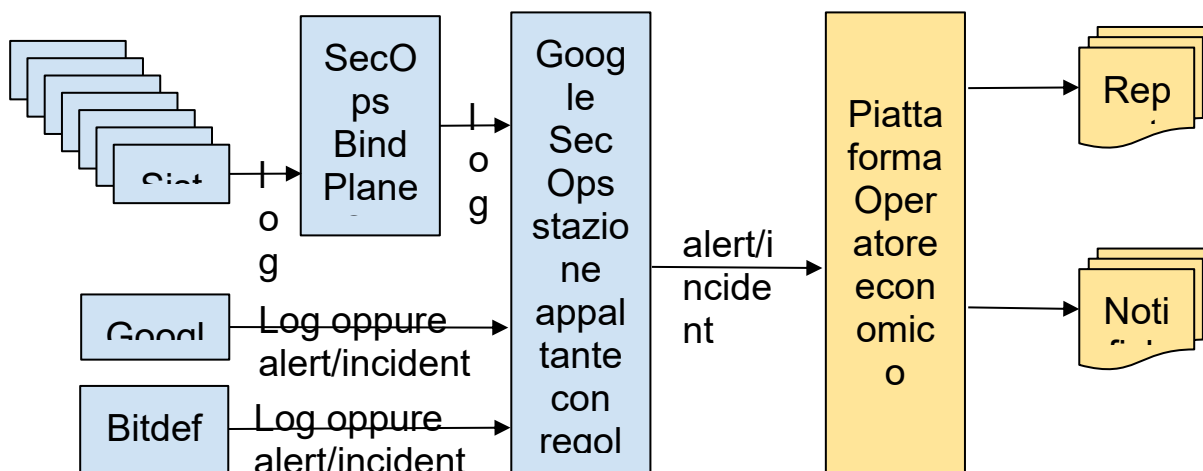
2. Oggetto

L'oggetto della presente procedura è l'affidamento di un servizio Security Operations Center (SOC) fornito in modalità "as a Service" che garantisca:

- Progetto di onboarding per le risorse UNIFI da monitorare
- Monitoraggio continuo 24x7 degli eventi di sicurezza provenienti dalle infrastrutture IT di UNIFI;
- Correlazione dei log attraverso l'utilizzo di piattaforma SIEM (Security Information and Event Management) Google SecOps della stazione appaltante e analisi degli incidenti e degli alert tramite la piattaforma suddetta o tramite piattaforma di Incident Management dell'operatore economico che potrà prelevare gli alert e/o i log dal SIEM della stazione appaltante.
- Rilevamento tempestivo delle minacce e degli incidenti di sicurezza (incident detection);
- Attivazione di contromisure di emergenza come da apposite procedure da condividere con l'Ateneo e rivedere periodicamente durante il servizio
- Classificazione e gestione degli incidenti (incident triage e incident response);
- Notifica tempestiva agli stakeholder di UNIFI degli eventi rilevanti;
- Supporto nell'analisi approfondita degli incidenti con suggerimenti per la remediation;
- Reportistica periodica sullo stato di sicurezza e sugli incidenti gestiti.

Il servizio dovrà integrarsi con l'infrastruttura Google SecOps indicata dalla stazione appaltante, garantendo la raccolta e l'analisi dei log provenienti dalle diverse fonti tecnologiche presenti nell'Ateneo.

L'architettura del servizio sarà indicativamente la seguente. L'operatore economico potrà avvalersi anche della piattaforma SecOps della stazione appaltante per erogare il servizio o di una propria piattaforma di incident management.



A valle dell'onboarding a servizio attivo, le regole di correlazione aggiunte durante l'erogazione del servizio per minimizzare i falsi positivi, limitare gli errori di detection o intercettare nuove minacce dovranno essere inserite sull'infrastruttura SIEM della stazione appaltante nei limiti dichiarati nella proposta tecnica.

Tutte le regole di correlazione create sul SIEM della stazione appaltante rimarranno in uso alla stazione appaltante anche al termine del contratto.

3. Caratteristiche del servizio

3.1 Progetto di onboarding

Il fornitore presenterà un progetto dettagliato di onboarding che sarà oggetto di valutazione tecnica, come specificato nel Disciplinare di gara.

Il progetto prevede:

preveda:

1. Analisi delle fonti dati presenti nell'infrastruttura UNIFI (server, firewall, endpoint, sistemi di identity & access management, apparati di rete, servizi cloud come Google workspace e EDR Bitdefender). Dovranno essere supportate le seguenti fonti log come minimo:
 - 1) Sistemi di Identity & Access Management (IAM) come Active directory, LDAP, sistemi IAM come CAS e Syncope.
 - 2) EDR: Endpoint con console in cloud BitDefender (workstation, server), anche limitatamente ai soli incident

- 3) Apparatati di rete (firewall in particolare Fortinet e Cisco, switch in particolare Cisco, router e log server a servizio di essi come syslog server e Fortianalyzer)
 - 4) Servizi cloud (Microsoft 365, Google Workspace)
 - 5) Sistemi application server come Tomcat e stack LAMP
 - 6) Sistemi di virtualizzazione (VMWARE)
 - 7) Database (Oracle, Postgresql e MariaDB/Mysql)
 - 8) Veeam Data Platform (Backup & Replication, VeeamOne, Recon Scanner e Orchestrator)
 - 9) Server Linux anche se non gestiti da EDR
 - 10) Server Windows anche se non gestiti da EDR
2. Pianificazione delle attività di integrazione delle fonti dati individuate con Google SecOps della stazione appaltante e con l'eventuale piattaforma di incident management dell'operatore economico;
 3. Definizione dei tempi massimi di onboarding per il raggiungimento della piena operatività del servizio con un limite massimo di 3 mesi con l'integrazione di 100 fonti on-premise (le fonti potranno essere anche meno di 100 nel caso in cui la stazione appaltante decida di integrarne meno), Google Workspace for education e piattaforma EDR in cloud
 4. Implementazione delle regole di correlazione su GoogleSecOps e loro manutenzione ed integrazione durante il periodo del servizio
 5. Piano di test e verifica della corretta ricezione e correlazione dei log.
 6. Piattaforma di incident management eventualmente utilizzata dall'operatore economico nel caso in cui decida di non avvalersi della piattaforma SIEM/SOAR della stazione appaltante per tale scopo con i dati collocati in datacenter che rientrino fra quelli permessi dal GDPR

3.2 Operatività 24x7

Il servizio SOC dovrà essere operativo 24 ore su 24, 7 giorni su 7, garantendo la presenza continuativa di security analyst qualificati per il monitoraggio, l'analisi e la risposta agli incidenti di sicurezza.

3.3 Personale dell'appaltatore

Il numero minimo di security analyst (figure specializzate nel monitoraggio, individuazione e mitigazione di incidenti cyber) dedicati al servizio SOC, anche se non dedicati al monitoraggio della sola stazione appaltante, non dovrà essere inferiore a 5.

3.4 SLA e performance operative

Si richiedono i seguenti livelli di servizio minimi attesi in relazione alla individuazione, classificazione, triage e notifica:

- **TTD (Time to Detect)**: presa in carico dell'incidente entro 2 ore
- **TTT (Time to Triage)**: classificazione (critico, alto, medio, basso) dell'incidente entro 4 ore
- **TTN (Time to Notify)**: notifica dell'incidente entro 8 ore per incidenti critici, 16 ore per incidenti di livello medio o alto e 24 ore per incidenti classificati come bassa priorità nel caso in cui tali incidenti siano stati indicati come da segnalare.

4. Importo e durata del servizio

L'importo a base d'asta è pari ad euro 600.000,00 + IVA.

L'importo degli oneri per la sicurezza da interferenze è pari a € 0,00 poiché considerate le caratteristiche del servizio, non si rilevano interferenze per le quali intraprendere misure di prevenzione e protezione finalizzate a eliminare o ridurre eventuali rischi, nello specifico il servizio consiste nel monitoraggio h24 tramite raccolta e correlazione di log, la rilevazione, l'analisi e la risposta agli eventi e agli incidenti di sicurezza informatica relativi all'infrastruttura ICT dell'Amministrazione.

La durata dell'appalto è di 4 anni decorrenti dalla data di sottoscrizione del contratto, con possibilità di rinnovo per ulteriori 4 anni.

Per i primi dodici mesi, decorrenti dalla data di stipula o dalla data del verbale di avvio di esecuzione del servizio, il contratto si intende conferito a titolo di prova.

Durante tale periodo, la stazione appaltante ha assoluta e libera facoltà di recedere unilateralmente e liberamente dal contratto in qualsiasi momento e per qualsiasi motivo, senza necessità di specificare la causa, mediante semplice comunicazione PEC da inviarsi all'operatore economico con un preavviso di almeno 15 giorni.

Il recesso avrà efficacia a partire dal giorno successivo alla scadenza del periodo di preavviso.

In caso di recesso, le Parti si impegnano a definire e regolare entro la data di efficacia del recesso ogni pendenza economica o prestazione in corso derivante dall'esecuzione del presente Contratto fino a quel momento. Restano comunque valide le eventuali clausole che per loro natura sono destinate a sopravvivere al recesso quali le clausole di riservatezza.

L'esercizio del diritto di recesso non darà diritto a indennizzi o risarcimenti a favore dell'operatore economico.

Le fasi del progetto e relativo servizio includono a titolo esemplificativo almeno le seguenti:

- FASE 1 (ONBOARDING): Da completare entro 3 mesi dall'avvio
 - progetto di onboarding
 - onboarding effettivo per un numero minimo di risorse come definito nel disciplinare e capitolato
 - Verifica delle fonti dati e della corretta ricezione dei log
 - Creazione delle regole di correlazione
 - Eventuale invio a piattaforma dell'operatore economico di alert
- FASE 2 (SERVIZIO):
 - Monitoraggio H24 allarmi
 - Integrazione regole di correlazione e playbook
 - Reportistica degli allarmi rilevati
 - triaging degli allarmi

5. Responsabile Unico del Progetto e Direttore dell'esecuzione

I servizi sono da effettuarsi in accordo con il Responsabile Unico del Progetto (RUP), Dott. Fabrizio Fioravanti. Ai sensi dell'art. 32 dell'All. II.14 del codice dei contratti, che individua i

contratti di servizi e forniture di particolare importanza, per qualità o importo delle prestazioni, verrà nominato il direttore dell'esecuzione.

6. Opzioni e modifiche al contratto

Eventuali modifiche del contratto saranno possibili nel rispetto di quanto disposto all'art. 120 del d.lgs. 36/2023.

Nessuna variazione o modifica al contratto può essere introdotta dall'esecutore, se non è disposta o concordata con il Direttore dell'esecuzione del contratto e/o con il RUP e preventivamente approvata dalla Stazione appaltante.

Le modifiche non previamente autorizzate non danno titolo a pagamenti o rimborsi di sorta.

7. Responsabile del servizio, obblighi e oneri dell'aggiudicatario

L'aggiudicatario dovrà nominare un Responsabile/Referente ai fini dell'esecuzione del servizio affidato dall'Università, comunicando tale riferimento e i relativi recapiti di contatto al RUP. Tale Responsabile, il quale dovrà garantire reperibilità, è autorizzato a trattare in nome e per conto dell'impresa qualsiasi questione relativa alla esecuzione del contratto.

L'operatore che risulterà affidatario sarà obbligato a rendere immediatamente noto alla Stazione Appaltante le seguenti situazioni in cui dovesse incorrere:

- modifica della ragione sociale del soggetto; cessione dello stesso; cessazione dell'attività;
- concordato preventivo, fallimento; stato di moratoria e di conseguenti atti di sequestro o pignoramento.

L'affidatario si impegna a:

- erogare il servizio sulla base di quanto stabilito nel presente Capitolato e nel successivo contratto;
- svolgere le attività oggetto del contratto in coordinamento con la Stazione Appaltante;
- sollevare e tenere indenne l'Università da qualsiasi responsabilità civile derivante dall'esecuzione del contratto, nei confronti dei terzi danneggiati e per eventuali conseguenti richieste di danni.

- segnalare nel più breve tempo possibile e comunque non oltre tre giorni dal suo verificarsi al Responsabile del Procedimento ed al Direttore dell'Esecuzione del Contratto qualunque evento che possa avere influenza sull'esecuzione del servizio
- rispettare la normativa comunitaria, nazionale e regionale vigente per le materie oggetto del presente appalto;
- garantire l'adempimento di tutti gli obblighi assicurativi e previdenziali previsti dalla normativa vigente a favore dei propri addetti alla realizzazione dell'attività;
- garantire che le strutture e le attrezzature messe a disposizione per lo svolgimento delle attività corrispondano ai requisiti delle vigenti normative in materia di idoneità e sicurezza;
- relazionare periodicamente e puntualmente sulle attività svolte durante il progetto di onboarding e con una reportistica sugli incidenti in corso di servizio;
- relazionare sulla conclusione delle attività di onboarding evidenziando le problematiche emerse, le soluzioni adottate, e quant'altro necessario a quantificare e qualificare il servizio fornito;
- garantire che gli operatori del SOC siano idonei alle mansioni di cui al presente Capitolato;
- farsi carico degli obblighi relativi alle vigenti disposizioni in materia di protezione dell'impiego e di condizioni di lavoro applicabili nel corso dell'esecuzione del contratto (sicurezza e protezione dei lavoratori, nonché delle condizioni di lavoro).

8 Modalità di pagamento

Il pagamento del corrispettivo sarà erogato con cadenza trimestrale previa predisposizione di tutti gli atti contabili di cui alla normativa vigente e acquisizione di tutti i controlli di legge previsti in materia di trasparenza, anticorruzione e regolarità amministrativa e contributiva. La Stazione Appaltante, previo accertamento da parte del DEC della regolare esecuzione delle prestazioni di cui al presente Capitolato, provvederà alla liquidazione delle somme spettanti entro 30 giorni dalla presentazione della fattura elettronica.

Eventuali contestazioni ed irregolarità sospenderanno tale termine.

Sulla fattura dovrà essere specificato:

- l'oggetto dell'appalto;
- il codice identificativo gara;
- il periodo di imputazione della spesa per la quale si chiede la liquidazione;
- il Codice Identificativo Univoco 5F1SMO

Il pagamento verrà disposto da parte dell'ufficio competente, a seguito di verifica di regolarità del/dei D.U.R.C. (documento unico di regolarità contributiva).

Le fatture sono soggette al regime dello "split payment" ai sensi della L. 190/2014, art. 1 co. 629, lett.b).

Nel caso di contestazione da parte dell'Università, per vizio o difformità di quanto oggetto del servizio rispetto al contratto, i termini di pagamento previsti nel presente articolo restano sospesi dalla data di spedizione della nota di contestazione e riprenderanno a decorrere con la definizione della pendenza.

Infine, nel caso in cui dal riscontro ordine/fattura emergessero delle divergenze, il Settore Finanziario provvederà a richiedere per iscritto al Fornitore ogni elemento utile alla chiusura della pratica liquidatoria. Detta richiesta interrompe il termine concordato per il pagamento delle fatture, che inizierà a decorrere nuovamente dalla data di ricevimento degli elementi richiesti secondo le indicazioni fornite.

La Stazione Appaltante potrà rivalersi, per ottenere la rifusione di eventuali danni contestati, il rimborso di spese ed il pagamento di penalità, mediante ritenuta da operarsi in sede di pagamento dei corrispettivi.

9. Revisione prezzi del servizio

È ammessa la revisione del prezzo d'appalto.

Qualora nel corso di esecuzione del contratto, al verificarsi di particolari condizioni di natura oggettiva, si determina una variazione, in aumento o in diminuzione, del costo del servizio superiore al cinque per cento dell'importo complessivo, i prezzi sono aggiornati automaticamente, nella misura dell'ottanta per cento del valore eccedente la variazione del 5 per cento applicata alle prestazioni da eseguire.

Ai fini della determinazione della variazione dei costi e dei prezzi si utilizzano gli indici dei prezzi alla produzione dei servizi e gli indici delle retribuzioni contrattuali orarie.

Associazione CPV 72500000-0 Servizi informatici all'indice ISTAT dei prezzi alla produzione dei servizi

https://esploradati.istat.it/databrowser/#/it/dw/categories/IT1,Z0400PRI,1.0/DCSC_PREZP_RODSERV_1

Riferimento tabella D.2

CPV	DESCRIZIONE CPV	TIPO INDICE	[ATECO/ECOICOP] INDICE ISTAT - I
72500000 -0	Servizi informatici	PPS	[62] Produzione di software, consulenza informatica e attività connesse

indice prevalente: PPS prezzi alla produzione dei servizi: indice ISTAT [62] Produzione di software, consulenza informatica e attività connesse.

procede al calcolo della variazione utilizzando la seguente formula:

$$V_t = (I_t - I_0) / I_0 \times 100$$

dove t = 0 corrisponde alla data di inizio del primo periodo di rilevazione e t = 1, 2, 3, t corrisponde alla data di fine del periodo di rilevazione considerato e I è l'indice utilizzato.

La Stazione appaltante monitorerà l'andamento degli indici di cui all'articolo 60 del Codice con frequenza trimestrale al fine di valutare se sussistono le condizioni per l'attivazione delle clausole di revisione prezzi.

Il RUP nei successivi 30 giorni dalla modifica dell'indice darà luogo alle operazioni di determinazione della variazione in ossequio all'art. 12 dell'Allegato II.2 bis. Una volta svolte le predette operazioni, la Stazione appaltante, previa comunicazione all'appaltatore dei prezzi revisionati, procederà al pagamento dei corrispettivi dovuti in conseguenza dell'applicazione della revisione prezzi entro i successivi 30 giorni.

Al verificarsi delle particolari condizioni di natura oggettiva indicate al primo capoverso, si applica la revisione dei prezzi anche ai contratti di subappalto e ai subcontratti comunicati alla stazione appaltante.

10. Garanzia definitiva

Prima della stipula del contratto, l'aggiudicatario è tenuto a costituire apposita garanzia definitiva, a norma dell'art. 53 del d.lgs. n. 36/2023, pari al 10 per cento dell'importo contrattuale. La garanzia può essere costituita mediante cauzione, come precisato nell'art. 106 del codice dei contratti, al quale si formula espresso rinvio, o con garanzia fideiussoria, anche in questo caso con le modalità specificate dal citato articolo 106, purché contenga la rinuncia all'eccezione di cui all'art. 1957, comma 2 del codice civile, preveda espressamente la rinuncia al beneficio della preventiva escussione del debitore principale, preveda l'operatività entro 15 giorni, a semplice richiesta della stazione appaltante.

Non verrà accettata altra forma di costituzione della garanzia definitiva.

Alla garanzia definitiva si applicano le riduzioni previste dall'articolo 106, comma 8, e gli aumenti previsti dall'articolo 117, comma 2.

La garanzia definitiva è progressivamente svincolata in funzione dell'avanzamento dell'esecuzione del contratto, nel limite massimo dell'80 per cento dell'importo garantito. L'ammontare residuo del 20 per cento è svincolato a conclusione del contratto, previo accertamento degli adempimenti, sulla base del certificato di verifica di conformità.

11. Responsabilità e assicurazione obbligatoria

Ogni responsabilità inerente all'esecuzione delle prestazioni oggetto del presente appalto fa interamente carico all'Appaltatore.

L'Appaltatore assume pertanto a proprio esclusivo carico ogni e qualsiasi responsabilità civile conseguente agli eventuali sinistri e/o danni, di tutti i generi, che possano derivare dall'esecuzione del servizio.

L'affidatario è obbligato a stipulare e mantenere attiva per tutta la durata dell'appalto polizze assicurative per la Rc Professionale tecnologica e per il rischio Cyber con primari istituti assicurativi, a copertura dei danni causati dagli eventi informatici sia dalla mancata erogazione del servizio da parte del fornitore .

La polizza dovrà prevedere un massimale non inferiore a € 500.000,00 per sinistro e per anno, e dovrà esplicitamente includere la copertura per danni da interruzione di servizio, violazione della privacy (GDPR) e danni da diffusione di malware/virus informatici.

12. Verifica di conformità

Il contratto è soggetto a verifica di conformità, per appurare che l'oggetto del contratto in termini di prestazioni, obiettivi e caratteristiche tecniche, economiche e qualitative sia stato realizzato ed eseguito nel rispetto delle previsioni e delle pattuizioni contrattuali.

13. Penali

Per ogni violazione degli obblighi derivanti dal presente Capitolato e per ogni caso di carente o incompleta esecuzione del servizio, la stazione appaltante, fatto salvo ogni risarcimento di maggiori ed ulteriori danni, potrà applicare alla Ditta appaltatrice delle penali, calcolate in misura giornaliera pari allo 0,5 per mille dell'ammontare netto contrattuale per i seguenti casi

- Per ogni incidente critico non rilevato entro i tempi previsti dallo SLA di detection;
- Per ogni ritardo nella notifica di incidenti critici superiore ai tempi previsti dallo SLA di notification;

e comunque non superiori, complessivamente, al 10 per cento di detto ammontare netto contrattuale; qualora le inadempienze siano tali da comportare una penale di importo superiore alla predetta percentuale il Responsabile promuove l'avvio delle procedure in materia di risoluzione del contratto

Il responsabile del progetto o il Direttore dell'esecuzione dispone l'applicazione delle suddette penali specificando l'importo. L'applicazione delle penali sarà preceduta da regolare contestazione scritta dell'inadempienza, a mezzo Posta Elettronica Certificata, avverso la quale la Ditta avrà facoltà di presentare le sue controdeduzioni entro 3 (tre) giorni dal ricevimento della contestazione stessa. Resta, in ogni caso, ferma la facoltà della stazione appaltante, in caso di gravi violazioni, di sospendere immediatamente il servizio alla Ditta appaltatrice e di affidarla anche provvisoriamente ad altra Ditta, con costi a carico della parte inadempiente ed immediata escussione della garanzia definitiva.

Il pagamento della penale dovrà essere effettuato entro 15 (quindici) giorni dalla notifica o dalla ricezione della comunicazione di applicazione. Decorso tale termine la stazione appaltante si rivarrà trattenendo la penale sul corrispettivo della prima fattura utile ovvero sulla garanzia definitiva. In tale ultimo caso la Ditta è tenuta a ripristinare il deposito

cauzionale entro 10 (dieci) giorni dalla comunicazione del suo utilizzo pena la risoluzione del contratto.

14. Tracciabilità dei flussi finanziari

Il contratto è soggetto alle disposizioni in tema di tracciabilità dei flussi finanziari di cui alla legge 13 agosto 2010, n. 136 e successive modificazioni, in merito ai quali l'aggiudicatario assume su di sé ogni obbligo di adempimento.

In ottemperanza alle disposizioni di cui alla medesima legge n. 136/2010 l'aggiudicatario procederà, quale condizione per consentire all'Università il pagamento dei corrispettivi, a comunicare in forma scritta gli estremi identificativi del conto corrente bancario/postale dedicato, anche in via non esclusiva, ai fini del transito dei movimenti finanziari relativi alla gestione dell'affidamento oggetto del presente Capitolato, nonché ad indicare le generalità e il Codice Fiscale delle persone delegate ad operare su tale conto.

L'aggiudicatario si obbliga, altresì, a comunicare tempestivamente qualsiasi modifica relativa ai dati trasmessi, esonerando l'Università da qualsiasi responsabilità derivante da pagamenti eseguiti sulla base dei riferimenti non aggiornati.

Il mancato utilizzo del bonifico bancario o postale ovvero degli altri strumenti idonei a consentire la piena tracciabilità delle operazioni finanziarie relative al presente affidamento costituisce, ai sensi dell'art. 3, comma 9 bis, della Legge n. 136/2010 e s.m.i., causa di risoluzione del contratto.

15. Subappalto e cessione del contratto

In ragione dell'elevata complessità delle prestazioni da eseguire si dispone il divieto di subappalto per il presente appalto. In particolare, è necessario che il servizio sia offerto come un unicum dallo stesso operatore economico per garantire il rispetto delle tempistiche di SLA e per evitare che la supply chain si allunghi aumentando il rischio cyber per l'allungamento della catena di fornitura sia per l'aumento dei tempi di identificazione e contenimento.

È assolutamente vietato, pena l'immediata risoluzione del contratto, la cessione totale o parziale, sotto qualsiasi forma, del contratto.

La cessione dei crediti derivanti dal contratto è ammessa, purché preventivamente notificata alla Stazione Appaltante e dalla medesima accettata.

16. Cause di risoluzione del contratto

La stazione appaltante può risolvere il contratto, oltre che nei casi contemplati dall'art. 122 del d.lgs. n. 36/2023, anche nelle ipotesi di seguito elencate.

In tutti i casi di risoluzione del contratto l'appaltatore ha diritto soltanto al pagamento delle prestazioni relative ai servizi regolarmente eseguiti.

Nelle ipotesi successivamente elencate, ogni inadempienza agli obblighi contrattuali sarà specificatamente contestata dal direttore dell'esecuzione o dal RUP a mezzo di comunicazione scritta, inoltrata via PEC al domicilio eletto dall'aggiudicatario. Nella contestazione sarà prefissato un termine non inferiore a 5 giorni lavorativi per la presentazione di eventuali osservazioni; decorso il suddetto termine, l'amministrazione, qualora non ritenga valide le giustificazioni addotte, ha facoltà di risolvere il contratto nei seguenti casi:

- frode nella esecuzione dell'appalto;
- mancato inizio dell'esecuzione dell'appalto nei termini stabiliti dal presente capitolato;
- mancato superamento del primo anno a titolo di prova;
- qualora si verifichino più di 5 superamenti degli SLA nell'anno di servizio;
- manifesta incapacità nell'esecuzione del servizio appaltato;
- inadempienza accertata alle norme di legge sulla prevenzione degli infortuni e la sicurezza sul lavoro;
- interruzione totale del servizio verificatasi, senza giustificati motivi, per 30 giorni anche non consecutivi nel corso dell'anno di durata del contratto;
- reiterate e gravi violazioni delle norme di legge e/o delle clausole contrattuali, tali da compromettere la regolarità e la continuità dell'appalto;
- cessione del contratto, al di fuori delle ipotesi previste;
- utilizzo del personale non adeguato alla peculiarità dell'appalto;
- concordato preventivo, fallimento, stato di moratoria e conseguenti atti di sequestro o di pignoramento a carico dell'aggiudicatario;

- inottemperanza agli obblighi di tracciabilità dei flussi finanziari di cui alla legge 13 agosto 2010, n. 136;
- ogni altro inadempimento che renda impossibile la prosecuzione dell'appalto, ai sensi dell'art. 1453 del codice civile.

Ove si verificassero deficienze e inadempimenti tali da incidere sulla regolarità e continuità del servizio, l'amministrazione potrà provvedere d'ufficio ad assicurare direttamente, a spese dell'aggiudicatario, il regolare funzionamento del servizio. Qualora si addingenga alla risoluzione del contratto, per le motivazioni sopra riportate, l'aggiudicatario, oltre alla immediata perdita della cauzione, sarà tenuto al risarcimento di tutti i danni, diretti ed indiretti ed alla corresponsione delle maggiori spese che l'amministrazione dovrà sostenere per il rimanente periodo contrattuale.

17. Recesso

L'amministrazione si riserva la facoltà, in caso di sopravvenute esigenze d'interesse pubblico, di recedere in ogni momento del contratto, con preavviso di almeno 20 (venti) giorni solari da notificarsi all'aggiudicatario tramite lettera raccomandata con avviso di ricevimento. In caso di recesso l'aggiudicatario ha diritto al pagamento da parte dell'amministrazione delle prestazioni eseguite, oltre al decimo delle prestazioni non eseguite, secondo quanto previsto dall'art. 123 del d.lgs. n. 36/2023 e del relativo allegato II.14.

18. Controversie

Le controversie aventi ad oggetto la validità, l'efficacia, l'interpretazione e l'esecuzione del presente Capitolato sono attribuite alla competenza esclusiva del Foro di Firenze.

È esclusa la devoluzione ad arbitri.

19. Stipula del contratto e relative spese

Il presente contratto è stipulato mediante scrittura privata in modalità elettronica, sottoscritto dalle parti con firma digitale.

Sono a carico della ditta appaltatrice le spese di bollo, scritturazione, copie di eventuali registrazioni e ogni altro onere necessario alla stipulazione del contratto. Il contraente dovrà corrispondere l'importo dell'imposta di bollo in conformità alla tabella di cui all'allegato I.4 del d.lgs. 36/2023.

20. Responsabilità dell'appaltatore

Ogni responsabilità inerente all'esecuzione delle prestazioni oggetto del presente contratto fa interamente carico all'Appaltatore. Nella responsabilità inerente all'esecuzione del servizio è altresì compresa la responsabilità per danni cagionati a terzi dall'Appaltatore stesso, in proprio o tramite il proprio personale, nel corso dell'esecuzione.

L'Appaltatore assume pertanto a proprio esclusivo carico ogni e qualsiasi responsabilità civile conseguente agli eventuali infortuni, sinistri e/o danni, di tutti i generi, che possano derivare dall'esecuzione del servizio.

21. Disposizioni in materia di sicurezza e documento di valutazione dei rischi interferenziali

L'operatore economico deve essere a conoscenza e rispettare il d.lgs. 81/2008 per tutto ciò che concerne la sicurezza e l'igiene sui luoghi di lavoro, nonché la restante normativa, anche regolamentare, generale e di settore, tenendo conto anche del regolamento di Ateneo, Rep. n. 401/2017 Prot. n. 79162 del 26/05/2017, rinvenibile al seguente link: <https://www.unifi.it/vp-2344-statuto-e-normativa.html>

L'operatore economico deve garantire che il personale individuato per le prestazioni oggetto del servizio sia formato in materia di sicurezza sul lavoro, garantendo la formazione, informazione e addestramento ai sensi dell'art. 36 e 37 del d.lgs. 81/2008.

Considerate le caratteristiche del servizio, non si rilevano interferenze per le quali intraprendere misure di prevenzione e protezione finalizzate a eliminare o ridurre eventuali rischi, consistendo il servizio nel monitoraggio h24 tramite raccolta e correlazione di log, la rilevazione, l'analisi e la risposta agli eventi e agli incidenti di sicurezza informatica relativi all'infrastruttura ICT dell'Amministrazione, quindi non è stato redatto il D.U.V.R.I.

22. Trattamento dati personali

I dati raccolti sono trattati e conservati ai sensi 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, del decreto legislativo 30 giugno 2003, n.196 recante il “Codice in materia di protezione dei dati personali” e ss mm e ii, del decreto della Presidenza del Consiglio dei Ministri n. 148/21 e dei relativi atti di attuazione. L’Università degli Studi di Firenze, ai sensi del regolamento (UE) del Parlamento europeo e del Consiglio, del 27 aprile 2016 e del Codice in materia di dati personali D.L. n.196/2003, informa l’Impresa che tratterà i dati, contenuti negli atti inerenti la pratica oggetto della presente procedura, esclusivamente per lo svolgimento delle attività e per l’assolvimento degli obblighi previsti dalle leggi e dai regolamenti aziendali in materia. Il titolare del trattamento dei Suoi dati personali è l’Università degli Studi di Firenze, con sede in Firenze, Piazza San Marco, 4 telefono 055 27571 e-mail: urp@unifi.it, pec: ateneo@pec.unifi.it

Il Responsabile della protezione dei dati (RPD) è il Dott. Massimo Benedetti, Dirigente dell’Area Affari generali e legali, Firenze, via G. la Pira, 4 telefono. 055 2757667 e-mail: privacy@adm.unifi.it

Il concorrente, essendo in possesso dei requisiti di esperienza, capacità ed affidabilità atti a garantire il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza, è idoneo ad assumere il ruolo di Responsabile del trattamento dei dati personali, ed è consapevole che, in caso di aggiudicazione della gara ed in corso di esecuzione contrattuale sarà nominato dall’Amministrazione “Responsabile” o “Sub Responsabile” del trattamento dei dati personali” per l’Amministrazione ai sensi dell’art. 28 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, contenente il Regolamento europeo sulla protezione dei dati (di seguito anche “Regolamento UE” o “GDPR”), nonché della normativa italiana di adeguamento al GDPR, previa verifica dei requisiti richiesti dalla disciplina vigente, nazionale e comunitaria da parte dell’Amministrazione. In tal caso, si impegna a presentare all’Amministrazione le garanzie e ad adottare tutte le misure tecniche e organizzative idonee ed adeguate ad adempiere alla normativa e regolamentazione in vigore sul trattamento dei dati personali e si impegna ad eseguire quanto necessario per ottemperare a qualsivoglia modifica delle Norme in materia di Trattamento dei Dati Personali applicabili al trattamento dei Dati Personali, che



generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali) per il Responsabile /Sub responsabile del trattamento dei dati personali collaborando, nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse, con il Titolare /Responsabile del trattamento affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti e alle nuove misure durante l'esecuzione del Contratto, senza oneri aggiuntivi a carico dell'Amministrazione