COMANDO OPERAZIONI IN RETE
UFFICIO AMMINISTRAZIONE
Sezione Contratti e Acquisti
C.F. 96451060584
Via Stresa 31/B – 00135 ROMA

Posta elettronica: cor@cor.difesa.it
Posta elettronica certificata: cor@postacert.difesa.it

Lettera di Ordinazione n. 113
(da citare in fattura)

Roma, 10/09/2025

Società NOBLEPROG ITALIA SRL
VIA MONTE NAPOLEONE 21 - 20121 - MILANO

Oggetto: **Gara 122 – Corso di formazione in ambito cooperazione internazionale per il progetto Cyber Forum 5+5 di Mitre Attack per i rappresentanti nazioni partecipanti. CIG: B83120699A- CUP D89J25000580001 - Capitolo 1269/1 - E.F. 2025. -TD 5568748.**

1. Codesta Ditta, si obbliga ad eseguire la sottonotata fornitura/prestazione, comprensiva dei relativi costi per la sicurezza, pari a euro 200,00 come da citata T.D.:

Descrizione	Quantità	Prezzo Unitario	Imponibile
Corso di formazione in ambito cooperazione internazionale per il progetto Cyber Forum 5+5 di Mitre Attack per i rappresentanti nazioni partecipanti, come da REQ. TEC. in allegato			€. 8.950,00
Esonero deposito cauzionale -1%			€. 89,50
Totale Imponibile			**€. 8.860,50**
IVA N/A			********
Totale			**€. 8.860,50**

2. La presenta commessa, per tutto quanto non previsto nella presente, si svolgerà sotto l'osservanza del d.lgs. 31 marzo 2023, n. 36 (*Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici*);

3. La Ditta si impegna ad eseguire la fornitura/prestazione a sua cura, rischio e spese **a decorrere dalla data di consegna/accettazione della presente e dovrà essere conclusa entro il giorno il 30/11/2025**, osservando tutte le norme e disposizioni indicate nella presente lettera di ordinazione.

4. Le clausole di revisione dei prezzi previste dall'articolo 60, comma 3 e comma 4, del Codice dei Contratti Pubblici, di cui al decreto legislativo 31 marzo 2023, nr. 36, si intendono parte integrante della presente scrittura. Per i contratti relativi ai lavori, in deroga all'articolo 60 del decreto legislativo n. 36 del 2023, le variazioni di prezzo dei singoli materiali da costruzione, in aumento o in diminuzione, sono valutate dalla stazione appaltante soltanto se tali variazioni risultano superiori al cinque per cento rispetto al prezzo, rilevato nell'anno di presentazione dell'offerta.

5. In caso di inadempimento ai patti e agli obblighi contrattuali l'A.D., fatto salvo quanto previsto dal codice dei contratti in ordine all'esecuzione in danno e alla risoluzione del rapporto contrattuale, applicherà una penalità del 1‰ (uno per mille) dell'importo contrattuale netto per ogni giorno di ritardo, fino al raggiungimento della percentuale massima del 10% (dieci per cento) dell'importo contrattuale netto.

6. **La fattura elettronica dovrà essere obbligatoriamente emessa in data successiva all'ultimazione della fornitura/servizio ovvero successivamente agli esiti positivi delle procedure previste ai fini dell'accertamento della conformità della fornitura/servizio (verbale di verifica conformità) e comunque, previa richiesta di autorizzazione al seguente indirizzo email: uam.sa.sca.cs@cor.difesa.it**, , ogni fattura dovrà essere compilata in maniera analitica nelle modalità richieste, come sopra specificato, e dovrà indicare il numero di protocollo del presente ordinativo e il numero di **CIG** e **CUP**, **la causale come da oggetto presente lettera e l'annotazione "SCISSIONE DEI PAGAMENTI".** La stessa dovrà essere intestata ed inviata a: COMANDO PER LE OPERAZIONI IN RETE – SERVIZIO AMMINISTRATIVO - Via Stresa, n. 31/b – 00135 ROMA Codice Fiscale 96451060584. **Codice Ufficio ai sensi dell'articolo 3, del Decreto MEF n. 55 del 3 aprile 2013 in materia di emissione, trasmissione e ricevimento della fattura elettronica 2SR075**.

7. La Ditta si obbliga al rispetto dei "Patti di integrità" sottoscritti in sede di presentazione dell'offerta ai sensi dell'art. 1 comma 17 Legge 190/2012. Tali provvedimenti, allegati al presente atto, ne costituiscono parte integrante, sostanziale, e pattizia ed il mancato rispetto degli stessi determinerà la risoluzione del presente atto negoziale.

8. Il pagamento, detratte le eventuali penalità di cui la Ditta si sia resa passibile, verrà effettuato, su presentazione di regolare fattura, dalla **Tesoreria Provinciale dello Stato**, a mezzo di bonifico on-line sul conto corrente bancario/postale che codesta Ditta avrà cura di comunicare nell'ambito della dichiarazione di cui alla legge 136/2010 in materia di tracciabilità dei flussi finanziari, previa verifica di buona esecuzione/collaudo ed accettazione di quanto richiesto; **Si precisa che il pagamento effettuato al netto dell'IVA ove applicabile entro il termine massimo di gg. 60 (sessanta) dalla data di presentazione della fattura. Esso è tuttavia subordinato all'esito positivo dell'accertamento effettuato sulla veridicità di quanto dichiarato in merito alla regolarità contributiva (DURC).**

9. **L'IVA, qualora dovuta, è a carico dell'Amministrazione Difesa e, ai sensi dell'art. 1 comma 629, lettera b), della Legge 190/2014, sarà trattenuta da questa Stazione Appaltante per il successivo versamento all'erario.**

10. Il presente affidamento trova copertura finanziaria con risorse attestate sul **capitolo di bilancio 1269/1 dell'E.F. 2025** mediante apertura di credito a favore del Funzionario Delegato dell'Ufficio Generale Centro di Responsabilità Amministrativa (UGCRA).

11. **La fornitura di eventuali materiali dovrà essere effettuata a cura di codesta Ditta presso il magazzino di questo Comando sito in Viale Castro Pretorio, 57 – 00185 Roma, indicando la codifica NATO dei materiali, previo contatto telefonico con il Mar.Ca. Alfredo MILITANO al seguente numero di telefono 06-46914523 - e-mail: consegnatario2@cor.difesa.it.**

12. **Direttore dell'Esecuzione Contrattuale (D.E.C.): S.T.V. RUFFO Sara tel. 0646912590 mail to: scd.cert.sthvii.add02@cor.difesa.it**.

13. Nell'ambito della fornitura oggetto del presente accordo/contratto, la Ditta si impegna ad operare nel rispetto delle politiche e procedure di sicurezza delle informazioni in essere presso l'Amministrazione e la sede stanziale di questa. L'Amministrazione sarà tenuta a mostrare all'operatore economico le predette politiche e procedure in caso di richiesta da parte dello stesso.

14. La Ditta si impegna a mantenere riservata, anche al termine del presente atto, qualsiasi informazione, sia essa in forma verbale, elettronica o cartacea, di cui venga a conoscenza durante o per l'erogazione del servizio/fornitura oggetto del presente contratto/ordine di acquisto.
La presente obbligazione di riservatezza non si applica alle informazioni che: (1) siano di dominio pubblico al momento della loro comunicazione; (2) siano state sviluppate autonomamente dalla Ditta; (3) siano divenute di dominio pubblico senza alcuna responsabilità da parte della Ditta, successivamente alla loro comunicazione da parte dell'Amministrazione alla Ditta; (4) siano già nella disponibilità della Ditta al momento della loro comunicazione da parte dell'Amministrazione e non siano gravate da alcun obbligo di riservatezza; (5) siano state comunicate a terzi da parte dell'Amministrazione senza alcun obbligo di riservatezza per i terzi; (6) siano state divulgate, per le quali l'Amministrazione ha espresso il suo consenso alla diffusione. In aggiunta a quanto sopra previsto, la Ditta può liberamente comunicare le suddette informazioni in caso di richieste derivanti da un'Autorità Giudiziaria. L'Amministrazione è a conoscenza del fatto che qualora la Ditta dovesse svolgere la propria attività commerciale nella ricerca e nell'analisi dei servizi I.T., la presente obbligazione di riservatezza non si applicherà ad ogni informazione ottenuta dalla Ditta attraverso ricerche, analisi, consulenze provenienti da fonti diverse dall'Amministrazione, ivi compresi i dipendenti che ricevono informazioni ai sensi del presente contratto.

15. **Nella fase di accertamento delle autocertificazioni, rese secondo quanto richiesto dall'articolo 94 del D.Lgs. 36 del 31 marzo 2023, nel caso di discordanza ovvero di dichiarazioni mendaci, il presente atto negoziale si riterrà unilateralmente annullato; inoltre questa stazione appaltante procederà alla prevista segnalazione all'Autorità Competente.**

IL RESPONSABILE UNICO DEL PROGETTO
IN FASE AFFIDAMENTO
Brig. Gen. Maurizio LAMBIASE
(Documento firmato digitalmente)

Firmato Digitalmente da/Signed by:
MAURIZIO LAMBIASE
RUP AFFID
In Data/On Date:
mercoledì 10 settembre 2025 16:39:44

FIRMA PER ACCETTAZIONE
IL LEGALE RAPPRESENTANTE DELLA DITTA
(Documento firmato digitalmente)

COMANDO PER LE OPERAZIONI IN RETE

Reparto Sicurezza e Cyber Defence

CERT Difesa

REQUISITO TECNICO OPERATIVO

Relativo a

Corsi di formazione nell'ambito della Cooperazione Internazionale
Evento CYBER Forum 5+5

Edizione 2025

Indice

1. Obiettivi

Il Comando per le Operazioni in Rete (COR), in accordo con le disposizioni discendenti dalle decretazioni emesse nel contesto del "*Board* Direttivo per il conseguimento degli obiettivi tecnologici funzionali all'evoluzione della nuova *Governance* di sicurezza della Difesa", ha identificato il CERT quale accentratore, gestore e valutatore di tutte le informazioni tecniche riguardanti le minacce cibernetiche nei confronti dell'intero comparto Difesa; ciò al fine di sviluppare una efficace azione di prevenzione e pronta reazione alle minacce attraverso l'impiego di adeguati strumenti di raccolta ed analisi delle informazioni relative ad attori malevoli e caratteristiche degli strumenti e delle modalità operative impiegate dagli stessi.

Nell'ambito dell'iniziativa 5+5 della Difesa, è stato istituito il "Cyber Forum", attraverso il quale i Paesi membri intendono cooperare nel campo della *Cyber Defence*.

Secondo quanto decretato da SMD, al COR è stata attribuita la competenza relativa all'organizzazione tecnico-logistica dell'evento. A tal proposito, è stato prevista attività formativa finalizzata ad incrementare la comune conoscenza della materia e la collaborazione in ambito cyber.

2. Riferimenti

- SMD-G-137/R - Tabelle Ordinative del Comando COR;
- SMD-I-013 - Procedure di risposta agli incidenti informatici riguardanti le reti telematiche della Difesa. Ed. 2008;
- SMD-I-024 - Procedure sulla gestione in sicurezza dei servizi informatici non-classificati dell'amministrazione difesa. Ed.2017 – aggiornata alle varianti 2020.
- Resoconto riunione Board attuativo del 07 marzo 2019;

3. Situazione *"AS IS"*

Considerata la concomitante evoluzione dei percorsi di crescita delle rispettive organizzazioni e la comune esigenza di approfondire le conoscenze nel dominio cibernetico, nonché di contrastare le crescenti fattispecie criminose in tal ambito, nel corso dell'evento 5+5 Cyber Forum - Cyber Commanders Committee 2025 sono stati programmati momenti formativi di particolare rilevanza, destinati ai rappresentanti nazionali ospitati.

4. Situazione *"TO BE"* / Oggetto della fornitura

Il presente requisito è mirato all'acquisizione del corso di formazione con programma e caratteristiche almeno equipollenti a quanto riportato in allegato e riepilogato come nella seguente tabella:

n.	Corso da fornire	Modalità di erogazione	Periodo	Prezzo unitario stimato da preventivo/online	Prezzo totale stimato da preventivo/online	Corsisti
1	MITRE ATT&CK	In presenza presso struttura della Difesa ubicata in Roma	Presumibilmente 11 e 12 novembre 2025	358 € / 683 €	8.950 € / 17.075 €	25

Nello specifico il corso dovrà essere:

- erogato in presenza presso la struttura della Difesa ubicata in Roma;
- della durata di n. 14 ore, suddiviso in n. 2 lezioni da tenersi in 2 giorni consecutivi, ciascuna della durata di n. 7 ore;
- corredato dei rispettivi laboratori, ove previsti;
- in lingua inglese;
- erogato nel mese di novembre 2025 (fatte salve eventuali necessità di carattere operativo che dovessero comportare la riprogrammazione da coordinare con la ditta aggiudicataria).

Qualora compresa, dovrà essere fornita la certificazione prevista per il completamento del corso. Alternativamente un attestato/diploma di partecipazione.

NobleProg corsi di formazione e consulenza

Domenico Tarsitani - Country Manager Italy | Procuratore
NobleProg® | The World's Locai Training Provider
Mob: +39 379 178 3195 | Email: domenico.tarsitani@nobleprog.com

NobleProg Italia S.R.L.
Via Monte Napoleone 21, 20121 Milan, Italy
C.F./P.I.: 13122000964 | Codice SDI: T9K4ZHO

Offerta Corso

MITRE ATT&CK

NobleProg

MITRE ATT&CK

Panoramica

MITRE ATT&CK è un framework ampiamente riconosciuto per la classificazione delle tattiche, tecniche e procedure (TTPs) utilizzate dagli attori malevoli durante un attacco informatico. Fornisce un modello strutturato per comprendere il comportamento degli avversari, identificare le vulnerabilità nei sistemi e dare priorità alle contromisure di sicurezza.

Questo corso intensivo di due giorni, erogato in modalità live con istruttore (online o in presenza), è pensato per analisti della sicurezza, SOC analyst, incident responder e professionisti IT interessati a integrare MITRE ATT&CK nei propri processi di difesa e analisi del rischio.

Obiettivi del corso

Al termine del corso, i partecipanti saranno in grado di:

- Comprendere la struttura e gli elementi fondamentali del framework MITRE ATT&CK.
- Configurare l'ambiente necessario per l'utilizzo pratico del framework.
- Classificare e analizzare le modalità operative degli aggressori informatici.
- Documentare i comportamenti degli avversari in ambienti reali.
- Correlare eventi di sicurezza utilizzando ATT&CK per migliorare la detection.
- Valutare l'efficacia delle misure di difesa esistenti e identificare le lacune da colmare.

Struttura del corso

- Lezioni teoriche con discussione guidata
- Numerosi esercizi pratici e scenari realistici
- Attività hands-on in un ambiente di laboratorio simulato

Personalizzazione

Il corso può essere personalizzato in base alle esigenze specifiche del team o dell'organizzazione. Per ulteriori informazioni o per una proposta su misura, contattaci direttamente.

Durata

14 ore, 2 giorni full-time

Prerequisiti

- Comprensione della sicurezza dei sistemi informativi

Descrizione del Corso

Questo corso intensivo di due giorni fornisce una panoramica pratica e approfondita del framework MITRE ATT&CK applicato al rilevamento e all'analisi dei malware. I partecipanti impareranno come classificare le minacce, utilizzare ATT&CK Navigator per tracciare tecniche e comportamenti degli attaccanti e analizzare scenari reali di compromissione.

Attraverso un approccio teorico-pratico, il corso guida i partecipanti nella preparazione di un ambiente operativo, nell'esecuzione di simulazioni di attacco e nella valutazione delle difese di sicurezza, con particolare attenzione alla documentazione delle falle e alla loro mitigazione.

1. Introduzione alla minaccia malware

- Cos'è il malware: definizione, obiettivi e impatti.
- Tipologie di malware: virus, worm, trojan, ransomware, spyware, adware, rootkit.
- Evoluzione del malware: da attacchi opportunistici a campagne mirate.
- Panoramica degli attacchi malware: esempi reali, cronologia e impatti documentati.

2. Modalità di propagazione del malware

- Malware non propagante: esecuzioni locali e mirate.
- Malware propagante: meccanismi di diffusione laterale, exploit di rete.
- Introduzione alle tecniche di attacco laterale e movimenti laterali.

3.11 framework MITRE ATT&CK

- Origine e struttura del framework MITRE ATT&CK.
- Matrici ATT&CK principali:
  - Enterprise ATT&CK
  - Pre-ATT&CK: fase di ricognizione e preparazione.
  - Mobile ATT&CK: minacce rivolte a dispositivi mobili.
  - Cloud e obliquo ATT&CK: ambienti ibridi e cloud-native.
- Differenze e complementarità tra le matrici.

4. Tattiche, Tecniche e Procedure (TTPs)

- Le 11 tattiche principali del framework (es. Initial Access, Execution, Persistence...).
- Tecniche associate e sottotecniche.
- Procedure note di attori di minaccia documentati.
- Come utilizzare ATT&CK per classificare e mappare un attacco reale.

5. Preparazione dell'ambiente di lavoro

- Installazione e configurazione di un ambiente sicuro di test.
- Version contro!: utilizzo di GitHub per gestire progetti e script.
- Download e analisi di un'applicazione tipo (To-Do list system).
- Installazione e configurazione di ATT&CK Navigator per la mappatura degli attacchi.

6. Simulazioni e laboratori pratici

Giorno 1: Analisi di un sistema compromesso tramite WMI

- Introduzione al Windows Management Instrumentation (WMI) come vettore di attacco.
- Esecuzione di script per simulare attacchi laterali.
- Identificazione e tracciamento della compromissione con ATT&CK Navigator.
- Monitoraggio del processo: strumenti e metodi.
- Documentazione delle tecniche osservate.
- Analisi dell'architettura di difesa e identificazione delle vulnerabilità.

Giorno 2: Compromissione tramite EternalBlue

- Panoramica sulla vulnerabilità EternalBlue (MS17-010).
- Simulazione dell'exploit in ambiente controllato.
- Analisi dei vettori di attacco utilizzati.
- Mappatura delle tecniche sul Navigator.
- Studio delle contromisure possibili e patching.
- Discussione guidata: impatto di EternaiBlue su sistemi legacy.

7. Sintesi e conclusioni

- Riepilogo dei concetti chiave appresi.
- Best practice per l'utilizzo continuo di MITRE ATT&CK in azienda.
- Come integrare ATT&CK nei processi di threat intelligence, incident response e gestione del rischio.
- Q&A finale con l'istruttore.

Metodologia didattica

- Lezioni teoriche supportate da esempi pratici.
- Attività hands-on su ambienti simulati.
- Analisi collaborativa di scenari reali.
- Materiale didattico e link a risorse aggiornate disponibili per tutti i partecipanti.

Quotazione del Corso

QUOTE REF	187259
TIPOLOGIA DEL CORSO	private | classroom
NOME DEL CORSO	*MITRE ATT&CK*
STRUTTURA DEL CORSO	https://www.nobleprog.it/cc/mitreattck
COURSE LANGUAGE	Italiano
DURATA	2 giorni, 7 ore al giorno, 14 ore in totale
DATA	11 - 12 Novembre 2025
PARTECIPANTI	25 (max 25)
PREZZO TOTALE	**Corso 7 000 EUR + LABs 1 950 EUR = 8 950 EUR (escl. IVA)** Prezzo partecipante: 358 EUR (corso) +78 EUR (LABs)
LUOGO DEL CORSO	Sede Cliente
PAGAMENTO	Modalità di pagamento: Carta di credito/debito o trasferimento bancario
COMMENTI	La quotazione è valida per 30 giorni. Le date saranno confermate dopo la prenotazione. La quotazione include: - Il corso - Personalizzazione contenuti - Materiale didattico - Condivisione risorse - DaDesktop LABs - E-certificates

Milano, 02/04/2025

Domenico Tarsitani - Country Manager Italy | Procuratore

NobleProg® | The World's Locai Training Provider

Mob: +39 379 178 3195 | Email: domenico.tarsitani@nobleprog.com

NobleProg Italia S.R.L.

Via Monte Napoleone 21, 20121 Milan, Italy

C.F./P.I.: 13122000964 | Codice SDI: T9K4ZHO

Firmato digitalmente da: DOMENICO TARSITANI
Luogo: Milano
Data: 29/07/2025 16:28:52

MINISTERO DELLA DIFESA
COMANDO PER LE OPERAZIONI IN RETE
PATTO DI INTEGRITA'

OGGETTO: **Gara 122 – Corso di formazione in ambito cooperazione internazionale per il progetto Cyber Forum 5+5 di Mitre Attack per i rappresentanti nazioni partecipanti. CUP D89J25000580001 - Capitolo 1269/1 - E.F. 2025.**

tra

il Comando per le Operazioni in Rete - Ufficio Amministrazione

e

la Ditta **NobleProg Italia S.R.L.** ..... (di seguito denominata Ditta), sede legale in **Milano**....., via **Monte Napoleone**.....n...**21**... codice fiscale/P.IVA **13122000964**....., rappresentata da **Tarsitani Domenico** ..... in qualità di .....**procuratore**.....

Il presente documento deve essere obbligatoriamente sottoscritto e presentato insieme all'offerta da ciascun partecipante alla gara in oggetto. La mancata consegna del presente documento, debitamente sottoscritto, comporterà l'esclusione automatica dalla gara.

VISTO

- la legge 6 novembre 2012 n. 190, art. 1, comma 17 recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione";
- il decreto legislativo 14 marzo 2013, n. 33 avente per oggetto il "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni";
- il decreto del Presidente della Repubblica 16 aprile 2013, n. 62 con il quale è stato emanato il "Regolamento recante il codice di comportamento dei dipendenti pubblici";
- il Protocollo d'intesa siglato tra il Ministero dell'Interno e l'Autorità Nazionale Anticorruzione il 15 luglio 2014;
- il decreto-legge 24 giugno 2014, n. 90 recante "Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari" convertito, con modificazioni, dalla legge 11 agosto 2014, n. 114;
- il Protocollo d'intesa siglato tra il Ministero dell'Interno e l'Autorità Nazionale Anticorruzione il 15 luglio 2014;
- il "Regolamento in materia di esercizio del potere sanzionatorio dell'Autorità Nazionale Anticorruzione per l'omessa adozione dei Piani triennali di prevenzione della corruzione, dei

Programmi triennali di trasparenza, dei Codici di comportamento" emanato dall'Autorità Nazionale Anticorruzione con delibera del 9 settembre 2014;

- il "Codice di comportamento dei dipendenti del Ministero della Difesa" approvato dal Ministro della Difesa il 22 marzo 2018;
- il Piano Nazionale Anticorruzione (P.N.A.) emanato dall'Autorità Nazionale Anticorruzione approvato con Delibera n. 1064 del 13 novembre 2019, e relativi allegati;
- il Piano Triennale di Prevenzione della Corruzione e della Trasparenza (PTPCT) 2025-2027 del Ministero della Difesa;

SI CONVIENE QUANTO SEGUE

Art. 1 - Il presente Patto d'integrità stabilisce la formale obbligazione della Ditta che, ai fini della partecipazione alla gara in oggetto, si impegna:

- a conformare i propri comportamenti ai principi di lealtà, trasparenza e correttezza, a non offrire, accettare o richiedere somme di denaro o qualsiasi altra ricompensa, vantaggio o beneficio, sia direttamente che indirettamente tramite intermediari, al fine dell'assegnazione del contratto e/o al fine di distorcerne la relativa corretta esecuzione;
- a segnalare alla stazione appaltante qualsiasi tentativo di turbativa, irregolarità o distorsione nelle fasi di svolgimento della gara e/o durante l'esecuzione dei contratti, da parte di ogni interessato o addetto o di chiunque possa influenzare le decisioni relative alla gara in oggetto;
- ad assicurare che non si è accordata e non si accorderà con altri partecipanti alla gara per limitare o eludere la concorrenza e, comunque, di non trovarsi in altre situazioni ritenute incompatibili con la partecipazione alle gare dal Codice degli Appalti, dal Codice Civile o dalle altre disposizioni normative vigenti;
- ad informare puntualmente tutto il personale, di cui si avvale, del presente Patto di integrità e degli obblighi in esso contenuti;
- a vigilare affinché gli impegni sopra indicati siano osservati da tutti i collaboratori e dipendenti nell'esercizio dei compiti loro assegnati;
- a denunciare alla Pubblica Autorità competente ogni irregolarità o distorsione di cui sia venuta a conoscenza per quanto attiene l'attività di cui all'oggetto della gara in causa.

Il legale rappresentante della Ditta, inoltre, dichiara: - di non aver conferito incarichi ai soggetti di cui all'art. 53, comma 16- ter, del D.Lgs.. n. 165 del 30 marzo 2001, così come integrato dall'art. 21 del D.Lgs. 8 aprile 2013 n. 39 e di non aver stipulato contratti di lavoro subordinato o autonomo con i medesimi soggetti; - di essere consapevole che, qualora emerga la violazione del suddetto divieto verrà disposta l'immediata esclusione dalla partecipazione alla procedura di affidamento.

Art. 2 - La Ditta prende nota e accetta che nel caso di mancato rispetto degli impegni anticorruzione assunti con il presente Patto di integrità, comunque accertato dall'Amministrazione, potranno essere applicate le seguenti sanzioni:

- esclusione del concorrente dalla gara;
- escussione della cauzione di validità dell'offerta;
- risoluzione del contratto;
- escussione della cauzione di buona esecuzione del contratto;
- esclusione del concorrente dalle gare indette dalla stazione appaltante per 5 anni.

Art. 3 – Fermo restando quanto previsto dai precedenti articoli 1 e 2, in aderenza alle prescrizioni in materia di anticorruzione contenute nel d.l. 90/2014 convertito dalla l. 114/2014 e ss.mm.ii.:

- la Ditta si impegna a dare comunicazione tempestiva alla Stazione appaltante di tentativi di concussione che si siano, in qualsiasi modo, manifestati nei confronti dell'imprenditore, degli

organi sociali o dei dirigenti di impresa. Il predetto adempimento ha natura essenziale ai fini della esecuzione del contratto. Ne consegue, pertanto, che il relativo inadempimento darà luogo alla risoluzione espressa del contratto stesso, ai sensi dell'art. 1456 c.c., qualora la mancata comunicazione del tentativo di concussione subito risulti da una misura cautelare o dal disposto rinvio a giudizio, nei confronti di pubblici amministratori che abbiano esercitato funzioni relative alla stipula ed esecuzione del contratto, per il delitto previsto dall'art. 317 c.p.;

- la Stazione appaltante si impegna ad avvalersi della clausola risolutiva espressa, di cui all'art. 1456 c.c., ogni qualvolta nei confronti dell'imprenditore o dei componenti la compagine sociale, o dei dirigenti dell'impresa, sia stata disposta misura cautelare o sia intervenuto rinvio a giudizio per taluno dei delitti di cui agli arti. 317 c.p., 318 c.p., 319 c.p., 319-bis c.p., 319- ter c.p., 319-quater c.p., 320 c.p., 322 c.p., 322-bis c.p., 346-bis c.p., 353 c.p. e 353-bis c.p..

Nei casi di cui al presente articolo, l'esercizio della potestà risolutoria da parte della Stazione appaltante è subordinato alla previa intesa con l'Autorità Nazionale Anticorruzione. La Stazione appaltante, pertanto, comunicherà la propria volontà di avvalersi della clausola risolutiva espressa al Responsabile per la prevenzione della corruzione che ne darà comunicazione all'Autorità Nazionale Anticorruzione. Quest'ultima potrà valutare se, in alternativa all'ipotesi risolutoria, ricorrano i presupposti per la prosecuzione del rapporto contrattuale tra Stazione appaltante ed impresa aggiudicataria, alle condizioni di cui al d.l. 90/2014.

Art. 4 - Il contenuto del Patto di integrità e le relative sanzioni applicabili resteranno in vigore sino alla completa esecuzione del contratto. Il presente Patto dovrà essere richiamato dal contratto quale allegato allo stesso onde formarne parte integrante, sostanziale e pattizia.

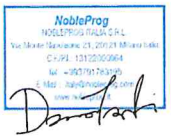
Art. 5 - Il presente Patto deve essere obbligatoriamente sottoscritto in calce ed in ogni sua pagina, dal legale rappresentante della Ditta partecipante ovvero, in caso di consorzi o raggruppamenti temporanei di imprese, dal rappresentante degli stessi e deve essere presentato unitamente all'offerta. La mancata consegna di tale Patto debitamente sottoscritto comporterà l'esclusione dalla gara.

Art. 6 - Ogni controversia relativa all'interpretazione ed esecuzione del Patto d'integrità fra la Stazione appaltante ed i concorrenti e tra gli stessi concorrenti sarà risolta dall'Autorità Giudiziaria competente.

Luogo e data Milano, **29/07/2025**

Per la Ditta:

Il legale rappresentante
(sottoscrizione digitale)



Firmato digitalmente
da: DOMENICO
TARSITANI
Luogo: Milano
Data: 29/07/2025
16:20:26

ALLEGATO 1

OGGETTO: Tracciabilità dei flussi finanziari - L. 136 del 13 agosto 2010, art. 3 (GURI n. 196 del 23 agosto 2010).

DICHIARAZIONE
(ex D.P.R. N.445 del 28 dicembre 2000)

In relazione a quanto in oggetto, il sottoscritto __**Domenico Tarsitani**_, nato a **Cagliari**, il **14/05/1990**, residente a **Cagliari** in via **San Benedetto n. 60**, in qualità di **procuratore** della **NobleProg Italia S.r.l**, sede legale in **Milano**, via **Monte Napoleone 21**, Partita IVA/C.F. **13122000964**

DICHIARA

- di assumere gli obblighi di tracciabilità dei flussi finanziari di cui all'art. 3, commi 7 e 8, della legge 13 agosto 2010, n. 136;
- di assumere gli obblighi connessi con l'identificazione dei lavoratori previsti dall'art. 18, comma 1, lettera n), del D.Lgs. 81/2008, così come integrato dall'art. 5 della legge n. 136/2010.

Istituto bancario: **Unicredit SPA**;

IBAN: **IT88K0200801760000106902501**;

ABI: **02008**;

CAB: **01760**;

C/c: **000106902501**;

CIN: **K**;

GENERALITA' DELEGATO/I AD OPERARE SUL CONTO:
- Nome **Eryk Krzysztof** cognome **Hajeki** cod. fisc. **HJCRKK88H23Z127B**

- Nome _____ cognome _____ cod. fisc. _____

- Nome _____ cognome _____ cod. fisc. _____

La società si impegna a comunicare all'Ente ogni eventuale variazione relativa al/i predetto/i conto/i corrente/i e ai soggetti autorizzati ad operare su di esso/i.

La società accetta che l'Ente provveda alla liquidazione del corrispettivo contrattuale, a mezzo bonifico bancario sull'Istituto di credito o su Poste Italiane S.p.A. e sul numero di conto corrente dedicato indicato nella presente clausola, secondo quanto disposto dal contratto in questione, sulla base della consuntivazione dei servizi/forniture effettivamente prestati.

Località, **Milano**

Timbro e firma

NobleProg

Firmato digitalmente da: DOMENICO TARSITANI
Luogo: Milano
Data: 29/07/2025 16:21:36

NobleProg