ARCAS
CYBERSECURITY LIFESTYLE

045 11171010
info@arcassecurity.it
arcassecurity.it

ARCAS S.R.L.

CONDIZIONI GENERALI DI ACQUISTO

per servizi di Cybersecurity, Consulenza Informatica, Penetration Testing e Software

Versione 1.0

Le presenti Condizioni Generali di Acquisto (di seguito "CGA") disciplinano i rapporti di fornitura relativi all'acquisto, da parte di ARCAS S.R.L. (di seguito "Società" o "Acquirente"), di beni, software, applicativi, licenze, servizi professionali, servizi gestiti, consulenza informatica, cybersecurity, vulnerability assessment, penetration testing, incident handling e servizi affini resi dal Fornitore. Le CGA si applicano agli Ordini di Acquisto e ai relativi contratti, salvo deroga espressa per iscritto.

1. OGGETTO E DOCUMENTI CONTRATTUALI

Il contratto è costituito, in ordine di prevalenza, da: (i) eventuale accordo quadro o contratto sottoscritto; (ii) Ordine di Acquisto o Statement of Work ("SOW"); (iii) allegati tecnici, SLA, regole di sicurezza, autorizzazioni, condizioni di licenza e accordi sul trattamento dei dati; (iv) presenti CGA. In caso di conflitto prevale il documento di livello superiore, limitatamente alle disposizioni espressamente derogate.

Le condizioni generali di vendita o altri documenti standard del Fornitore non si applicano, salvo espressa accettazione scritta della Società.

2. DEFINIZIONI

Per "Fornitore" si intende il soggetto che presta servizi o fornisce beni o software alla Società. Per "Software/Applicativo" si intende qualsiasi programma, piattaforma, componente, agente, libreria, firmware, servizio SaaS o altro prodotto software fornito, concesso in licenza o reso disponibile dal Fornitore.

Per "Servizi" si intendono le attività descritte nell'Ordine o nel SOW. Per "Cliente Finale" si intende, ove applicabile, il cliente della Società presso il quale o per il quale il Fornitore opera.

Per "Informazioni Riservate" si intendono dati, credenziali, configurazioni, log, report, codice, architetture, vulnerabilità, informazioni commerciali e ogni altra informazione non pubblica. Per "Dati Personali" valgono le definizioni del GDPR. Per "Ambito Autorizzato" si intende esclusivamente l'insieme di sistemi, domini, indirizzi, account, applicazioni, sedi e finestre temporali indicati per iscritto.

Per “Deliverable” si intende ogni report, documento, analisi, configurazione, script, codice o altro output prodotto dal Fornitore nell’esecuzione dei Servizi.

3. ORDINI, ACCETTAZIONE E MODIFICHE

Ogni Ordine dovrà indicare, ove applicabile, oggetto, Software/Applicativo e relativa versione, licenza e diritti d’uso, deliverable, corrispettivi, tempi, requisiti tecnici, referenti, SLA, requisiti di sicurezza e criteri di accettazione.

Il Fornitore conferma l’Ordine entro 5 (cinque) giorni lavorativi. L’avvio delle attività, la consegna di beni o software, la messa a disposizione dell’Applicativo o l’emissione della fattura costituiscono accettazione dell’Ordine.

Qualsiasi modifica, attività extra, variazione di prezzo, variazione di licenza o estensione dell’Ambito Autorizzato richiede la preventiva approvazione scritta della Società.

4. ESECUZIONE DEI SERVIZI E PERSONALE

Il Fornitore esegue i Servizi con diligenza professionale, secondo le migliori pratiche applicabili e con personale qualificato e adeguato alla natura delle attività.

Il Fornitore comunica tempestivamente assenze, sostituzioni, conflitti di interesse o impedimenti relativi alle risorse assegnate. Il personale resta alle dipendenze e sotto l’esclusiva responsabilità del Fornitore.

Il Fornitore risponde degli atti e delle omissioni di dipendenti, collaboratori e subfornitori.

5. SOFTWARE E APPLICATIVI FORNITI E INSTALLATI DALLA SOCIETÀ

Il Software/Applicativo dovrà essere conforme alle specifiche tecniche, funzionali e di sicurezza indicate nell’Ordine, nel SOW e nella documentazione contrattuale. Il Fornitore garantisce di avere tutti i diritti necessari per concedere la licenza o fornire il Software/Applicativo.

Prima della consegna, il Fornitore dovrà comunicare almeno: versione e release, requisiti hardware e software, sistemi operativi supportati, dipendenze, porte e protocolli utilizzati, privilegi richiesti, componenti di terze parti, modalità di autenticazione, eventuale telemetria, connessioni verso servizi esterni e requisiti di rete necessari all'installazione e al funzionamento.

Il Software/Applicativo non dovrà contenere funzionalità intenzionalmente malevole, backdoor, meccanismi di accesso non documentati, credenziali preimpostate non autorizzate o codice finalizzato a compromettere la sicurezza, la riservatezza o la disponibilità dei sistemi della Società o del Cliente Finale.

Il Fornitore dovrà informare preventivamente la Società di eventuali componenti open source o di terze parti soggetti a condizioni di licenza che possano imporre obblighi di divulgazione, modifica, distribuzione o altro vincolo sull'utilizzo del Software/Applicativo.

Il Fornitore dovrà mantenere e fornire, ove applicabile, la documentazione tecnica, le istruzioni di installazione, configurazione, aggiornamento, backup, rollback e disinstallazione. L'installazione eseguita dalla Società non esonera il Fornitore dalla responsabilità per difetti, incompatibilità o non conformità imputabili al Software/Applicativo o alla documentazione fornita.

Il Fornitore garantisce che il Software/Applicativo sarà sottoposto a ragionevoli controlli di sicurezza prima della consegna e si impegna a comunicare tempestivamente vulnerabilità note che possano incidere sul prodotto o sulla versione fornita.

Il Fornitore dovrà rendere disponibili, secondo quanto previsto dall'Ordine o dal relativo SLA, patch correttive e aggiornamenti di sicurezza per tutta la durata del periodo di supporto. Eventuali end-of-life, end-of-support o modifiche sostanziali al ciclo di vita dovranno essere comunicati con congruo preavviso.

Il Fornitore non potrà introdurre, senza preventiva approvazione scritta, modifiche che comportino nuove comunicazioni verso sistemi esterni, raccolta di dati, telemetria, aumento dei privilegi richiesti, nuove dipendenze critiche o modifiche sostanziali al modello di sicurezza.

Qualora il Software/Applicativo sia installato presso un Cliente Finale della Società, il Fornitore dovrà rispettare anche le istruzioni e i requisiti di sicurezza comunicati dalla Società per quel Cliente. Il rapporto contrattuale e commerciale con il Cliente Finale resta in capo alla Società, salvo diverso accordo scritto.

Salvo diverso accordo scritto, il Fornitore dovrà fornire supporto tecnico ragionevole per la diagnosi di errori di installazione, configurazione e funzionamento, inclusa la collaborazione necessaria per individuare se un malfunzionamento dipenda dal Software/Applicativo o dall'ambiente di installazione.

6. PENETRATION TEST, VULNERABILITY ASSESSMENT E ATTIVITÀ INTRUSIVE

Nessuna attività di scansione, test, exploit, social engineering, accesso remoto, raccolta di evidenze o trattamento di dati potrà iniziare senza un'autorizzazione scritta che definisca l'Ambito Autorizzato, le tecniche consentite, le esclusioni, le finestre operative, i contatti di emergenza e le regole di ingaggio.

Il Fornitore opera esclusivamente nell'Ambito Autorizzato e non può svolgere attività su sistemi, reti o applicazioni di terzi salvo che la Società dichiari per iscritto di disporre delle necessarie autorizzazioni.

Il Fornitore applica il principio di minima intrusività. Non esegue denial of service, distruzione, persistenza o esfiltrazione reale, salvo autorizzazione esplicita e specifica.

Il Fornitore deve interrompere immediatamente le attività in caso di rischio non previsto, malfunzionamento, indisponibilità dei sistemi o richiesta della Società.

La Società si impegna a fornire o procurare le autorizzazioni di propria competenza. Il Fornitore non deve presumere l'esistenza di autorizzazioni ulteriori e deve sospendere l'attività se l'autorizzazione risulta assente, ambigua o scaduta.

7. SICUREZZA DELLE INFORMAZIONI

Il Fornitore adotta misure tecniche e organizzative adeguate al rischio, incluse, ove pertinenti, autenticazione forte per accessi privilegiati, account nominativi, segregazione degli ambienti, cifratura, gestione delle vulnerabilità e patching, logging, backup, formazione e procedure di risposta agli incidenti.

Le credenziali fornite dalla Società non possono essere condivise o riutilizzate. Il Fornitore non può copiare, conservare o trasferire informazioni della Società su dispositivi personali o servizi non autorizzati.

Qualsiasi incidente, accesso non previsto, compromissione, perdita di dati o esposizione di credenziali deve essere comunicato senza ritardo e comunque entro 24 ore dalla conoscenza; le vulnerabilità critiche con rischio imminente devono essere comunicate immediatamente.

8. PROTEZIONE DEI DATI PERSONALI

Qualora il Fornitore tratti Dati Personali per conto della Società o di un Cliente Finale, le Parti sottoscrivono, ove necessario, un accordo ai sensi dell'art. 28 GDPR.

Il Fornitore tratta i dati esclusivamente su istruzioni documentate, garantisce la riservatezza delle persone autorizzate, assiste la Società negli adempimenti applicabili e cancella o restituisce i dati alla cessazione del rapporto.

Il ricorso a sub-responsabili che trattino Dati Personali richiede preventiva autorizzazione della Società.

9. SUBFORNITORI, FREELANCE, CLOUD, SAAS E AI

Il ricorso a subfornitori, freelance, piattaforme cloud, servizi SaaS, strumenti di scansione o sistemi di intelligenza artificiale che possano trattare informazioni della Società richiede preventiva autorizzazione scritta.

Il Fornitore resta pienamente responsabile dell'operato dei soggetti autorizzati e deve imporre loro obblighi almeno equivalenti in materia di riservatezza, sicurezza, protezione dei dati, proprietà intellettuale e continuità operativa.

Il Fornitore non può cedere il Contratto, in tutto o in parte, senza il preventivo consenso scritto della Società.

10. DELIVERABLE, SOFTWARE, COLLAUDO E ACCETTAZIONE

I Deliverable devono essere completi, accurati, verificabili e conformi all'Ordine o al SOW.

Per Software/Applicativi installati dalla Società, l'Ordine o il SOW potrà prevedere un periodo di collaudo e specifici criteri di accettazione. La messa a disposizione o l'installazione non costituisce di per sé accettazione definitiva.

La Società può contestare un Deliverable o un Software/Applicativo non conforme entro 15 (quindici) giorni lavorativi dalla consegna, dal completamento dell'installazione o dalla scoperta del difetto, ove non immediatamente rilevabile. Il Fornitore dovrà correggere o integrare senza costi aggiuntivi entro un termine ragionevole concordato.

Il pagamento non costituisce accettazione dei Servizi, del Software/Applicativo o dei Deliverable e non preclude i diritti della Società per difformità, vizi o vulnerabilità imputabili al Fornitore.

Il Fornitore dovrà collaborare, ove richiesto, alla risoluzione di problemi di interoperabilità tra il proprio Software/Applicativo e l'ambiente tecnico indicato nell'Ordine, purché conforme ai requisiti dichiarati dal Fornitore.

11. LICENZE E PROPRIETÀ INTELLETTUALE

Ciascuna Parte conserva la proprietà del proprio know-how, software, metodologie, strumenti e materiali preesistenti.

Per i Software/Applicativi concessi in licenza, la licenza dovrà essere chiaramente definita nell'Ordine o nel contratto, con indicazione almeno di durata, numero di utenti o installazioni, ambienti autorizzati, eventuali limiti territoriali, modalità di rinnovo e condizioni di supporto.

Salvo diverso accordo scritto, i Deliverable specificamente sviluppati per la Società, inclusi report, analisi, configurazioni, script personalizzati e documentazione, sono trasferiti alla Società al pagamento dei corrispettivi, con cessione dei diritti patrimoniali nella misura consentita dalla legge.

Il Fornitore conserva gli strumenti generici e il know-how residuo, ma non può riutilizzare Informazioni Riservate o dati identificabili della Società o dei Clienti Finali.

Il Fornitore garantisce di avere i diritti necessari per fornire il Software/Applicativo e che i Servizi e i Deliverable non violino diritti di proprietà intellettuale di terzi; terrà indenne la Società dalle relative pretese imputabili al Fornitore.

12. RISERVATEZZA E COMUNICAZIONI PUBBLICHE

Il Fornitore utilizza le Informazioni Riservate esclusivamente per l'esecuzione del Contratto e limita l'accesso al personale che ne abbia effettiva necessità.

L'obbligo di riservatezza permane per tutta la durata del rapporto e per 5 (cinque) anni successivi alla cessazione. Per credenziali, vulnerabilità non pubbliche, segreti commerciali e Dati Personali permane finché l'informazione non divenga legittimamente pubblica o non cessi l'obbligo di legge.

È vietato pubblicare, presentare, utilizzare in case study o comunicazioni commerciali, o comunque divulgare informazioni relative alla Società o ai Clienti Finali, nonché utilizzare nomi, marchi o loghi, senza previo consenso scritto.

13. CONTINUITÀ OPERATIVA, INCIDENTI ED EXIT MANAGEMENT

Il Fornitore mantiene piani proporzionati di continuità operativa e disaster recovery, ove pertinenti ai Servizi o al Software/Applicativo.

Il Fornitore coopera nelle attività di risposta, analisi, contenimento e ripristino degli incidenti e fornisce, ove richiesto, aggiornamenti ed evidenze.

Alla cessazione del rapporto, il Fornitore restituisce o cancella informazioni, credenziali, asset e dati della Società e disattiva i propri accessi. Su richiesta, fornisce attestazione dell'avvenuta restituzione o cancellazione.

Per Software/Applicativi, alla cessazione il Fornitore deve fornire, ove necessario, le informazioni utili alla migrazione, disinstallazione o sostituzione, inclusa la documentazione tecnica ragionevolmente necessaria.

14. GARANZIE, RESPONSABILITÀ E MANLEVA

Il Fornitore garantisce che i Servizi saranno eseguiti a regola d'arte, da personale qualificato, in conformità all'Ordine, alle leggi applicabili e alle regole di sicurezza concordate.

Per il Software/Applicativo il Fornitore garantisce la conformità alle specifiche concordate, la disponibilità dei diritti necessari alla licenza, l'assenza di funzionalità malevole intenzionali e la gestione delle vulnerabilità note secondo gli obblighi contrattuali.

Il Fornitore non garantisce l'assenza assoluta di vulnerabilità, ma garantisce la completezza e accuratezza professionale delle attività svolte e la corretta evidenziazione di limiti e assunzioni.

Il Fornitore risponde dei danni diretti derivanti da attività svolte fuori dall'Ambito Autorizzato, dalla violazione delle regole di ingaggio, da dolo, colpa grave, negligenza o imperizia, nonché dagli inadempimenti imputabili al Fornitore o ai suoi subfornitori.

Il Fornitore tiene indenne e manlevata la Società da pretese, danni, sanzioni, costi e spese derivanti da violazioni imputabili al Fornitore o ai suoi subfornitori, dalla violazione di diritti di terzi, dalla perdita o divulgazione illecita di informazioni o da attività non autorizzate.

Eventuali limitazioni di responsabilità potranno essere definite nell'Ordine o nel contratto specifico; restano in ogni caso ferme le responsabilità che non possono essere limitate per legge.

15. ASSICURAZIONE

Il Fornitore mantiene per tutta la durata del rapporto polizze adeguate alla natura dei Servizi e dei Software/Applicativi forniti, incluse, ove pertinenti, responsabilità civile professionale (Errors & Omissions), cyber liability e responsabilità connesse al trattamento dei dati.

Su richiesta, il Fornitore fornisce copia delle polizze o dei certificati assicurativi in corso di validità.

16. CORRISPETTIVI, SPESE, FATTURE E PAGAMENTI

I corrispettivi sono quelli indicati nell'Ordine o nel SOW e includono ogni costo necessario all'esecuzione dei Servizi e alla fornitura del Software/Applicativo, salvo diversa indicazione scritta.

Le spese sono rimborsabili esclusivamente se preventivamente autorizzate per iscritto e adeguatamente documentate.

Le fatture devono riportare il numero dell'Ordine, la descrizione dei Servizi, delle licenze o dei prodotti effettivamente forniti e il periodo di riferimento. Il pagamento avviene entro 60 giorni fine mese data fattura, salvo diverso accordo scritto.

La Società può contestare e sospendere la parte controversa di una fattura e compensare, nei limiti consentiti dalla legge, crediti liquidi ed esigibili.

17. DURATA, RECESSO E RISOLUZIONE

La durata è quella indicata nell'Ordine o nel SOW.

La Società può recedere da un Ordine o contratto a tempo indeterminato con preavviso di [30] giorni, corrispondendo quanto maturato per le attività correttamente eseguite fino alla cessazione.

Ciascuna Parte può risolvere il Contratto per grave inadempimento non sanato entro 15 giorni dalla diffida, salvo i casi in cui sia prevista la risoluzione immediata.

La Società può risolvere con effetto immediato, ove consentito dalla legge e dal contratto, in caso di grave violazione di sicurezza o riservatezza, trattamento illecito di dati, attività non autorizzata, subfornitura non autorizzata, perdita dei requisiti necessari, insolvenza o violazione grave degli obblighi di compliance.

18. FORZA MAGGIORE

Nessuna Parte risponde di ritardi o inadempimenti dovuti a eventi imprevedibili e fuori dal ragionevole controllo, purché ne dia comunicazione entro 3 giorni lavorativi, mitighi gli effetti e continui ad adempiere agli obblighi non impediti.

Non costituiscono forza maggiore la carenza ordinaria di personale, fondi, licenze o risorse, né l'inadempimento di un subfornitore salvo che l'evento sia a sua volta qualificabile come forza maggiore.

Se l'impedimento dura oltre 30 giorni, la Società può ridurre o risolvere l'Ordine senza ulteriori oneri, fatti salvi i diritti maturati.

19. COMPLIANCE, ETICA E CONDOTTA

Il Fornitore rispetta tutte le leggi e i regolamenti applicabili, inclusi quelli in materia di lavoro, anticorruzione, sanzioni, export control, sicurezza informatica, privacy e proprietà intellettuale.

Il Fornitore non offre né accetta vantaggi indebiti, segnala tempestivamente conflitti di interesse e mantiene documentazione idonea a dimostrare la conformità. Ove richiesto, collabora a ragionevoli verifiche della Società.

Qualora adottati, il Fornitore si impegna a rispettare i principi del Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001 e del Codice Etico della Società.

20. LEGGE APPLICABILE E FORO

Il Contratto è regolato dalla legge italiana. Le Parti tentano in buona fede una soluzione negoziale delle controversie.

Salvo diverso accordo scritto, è competente in via esclusiva il Foro di Verona, con facoltà della Società di agire anche presso il foro del Fornitore, nei limiti consentiti dalla legge.

21. DISPOSIZIONI FINALI

Il Contratto costituisce l'intero accordo tra le Parti sul relativo oggetto. Modifiche e deroghe sono valide solo se effettuate per iscritto da rappresentanti autorizzati.

L'eventuale invalidità o inefficacia di una disposizione non pregiudica la validità delle restanti disposizioni.

Restano efficaci anche dopo la cessazione del rapporto, per quanto applicabile, gli obblighi relativi a riservatezza, sicurezza, protezione dei dati, proprietà intellettuale, responsabilità, pagamenti maturati e legge applicabile.