# BluJay - Allegato sulla sicurezza delle informazioni

## 1. GENERALITÀ

Il presente Allegato sulla sicurezza delle informazioni di questa azienda ("**Allegato**") descrive i requisiti logici e fisici di sicurezza generalmente applicabili allo svolgimento di servizi per, o alla fornitura di servizi o prodotti a, Clienti a fronte del Contratto ("**Requisiti di sicurezza**") da parte dell'Azienda. Tranne che se diversamente previsto nel Contratto, i termini del presente Allegato avranno la precedenza e prevarranno su eventuali clausole in conflitto o incoerenti previste dal Contratto. Fermo restando, tuttavia, che ogni eventuale controllo di sicurezza specificato nel Contratto avrà la precedenza e prevarrà sulle clausole del presente Allegato qualora (i) il Contratto lo preveda espressamente o (ii) i controlli di sicurezza previsti nel Contratto superino quelli descritti nel presente Allegato.

## 2. DEFINIZIONI

(i) "**Personale aziendale**" significa i dipendenti e gli appaltatori dell'Azienda.

(ii) "**Dati riservati del cliente**" significa i dati definiti come "Informazioni riservate" ai sensi del Contratto e qualunque Informazione personalmente identificabile incluse, in modo non esaustivo, le Informazioni personali sensibili.

(iii) "**Dati del cliente**" significa qualunque dato trasmesso dal Cliente o dai suoi utenti autorizzati all'Azienda oppure utilizzati o acquisiti dell'Azienda in relazione alla fornitura di Servizi nell'ambito del Contratto.

(iv) "**Sistemi del cliente**" significa i sistemi del Cliente, gestiti dal Cliente e a cui l'Azienda accede in relazione alla fornitura di Software e/o Servizi. Includono sistemi computerizzati, software, reti, la tecnologia e i dati memorizzati su o accessibili attraverso l'utilizzo di tali sistemi, software e reti.

(v) "**Uso improprio di dati**" significa l'esercizio inappropriato o illecito del diritto o privilegio, come il diritto o il privilegio di accedere a informazioni, la divulgazione illecita di tali informazioni o l'esecuzione malevola o altrimenti impropria di una funzione o di una operazione.

(vi) "**Standard di settore**" significa qualunque delle seguenti condizioni:

(A) Utilizzato o adottato da un numero considerevole di aziende confrontabili in quanto dimensioni, levatura, funzione dell'Azienda.

(B) Prescritto per l'uso da un organismo di standardizzazione applicabile e riconosciuto a livello nazionale.

(C) Valutato come accettabile e ragionevole da un numero significativo di esperti riconosciuti del campo, tranne quando una recente divulgazione/scoperta pubblica ne riveli difetti/vulnerabilità sostanziali.

(vii) "**Perdita**" significa la perdita di controllo su Informazioni riservate, tale per cui uno o più attori possano ulteriormente divulgarle o farne un uso improprio.

(viii) "**Utente privilegiato**" significa qualunque utente che abbia una superiore autorità per avere accesso e configurare sistemi di rete, fra cui, in modo non esaustivo, amministratori di sistema e "super user" che possano distribuire, installare, aggiornare o modificare credenziali, sistemi operativi, codice sorgente, applicazioni e altri sistemi di rete.

(ix) "**Informazioni personali sensibili**" significa informazioni che identifichino o mettano in relazione un individuo identificabile (cioè una persona che possa essere identificata, direttamente o indirettamente, per esempio tramite riferimento a un numero di identificazione, dati sulla posizione, identificatore online oppure uno o più fattori specifici dell'identità fisica, fisiologica, mentale, economica, culturale o sociale della persona)e tali simili dati, regolati dalle leggi vigenti.

## 3. POLITICHE, CONSAPEVOLEZZA E FORMAZIONE

(a) L'Azienda gestisce, pubblica internamente e applica politiche e standard di sicurezza documentati relativi ai concetti fondamentali della sicurezza delle informazioni, fra cui clausole che richiedono la valutazione di vari rischi, vulnerabilità e pericoli relativi alla sicurezza delle informazioni, insieme alla gestione di tali rischi per soddisfare tali requisiti e rispettare tutte le leggi e le normative vigenti sulla protezione dei dati.

(b) L'Azienda gestisce un completo programma scritto sulla sicurezza delle informazioni, aggiorna e/o rivede tale programma, in base alle necessità, con una frequenza almeno annuale. L'Azienda contribuisce a garantire che tale programma (x) rispetti le leggi vigenti e sia allineato con gli Standard di settore applicabili, (y) includa le appropriate salvaguardie amministrative, logiche, tecniche e fisiche che rispettino il presente Allegato, (z) sia ragionevolmente progettato per raggiungere i seguenti obiettivi:

(A) Contribuire a garantire la riservatezza, l'integrità e la disponibilità dei Dati del cliente.

(B) Proteggere da qualunque minaccia o pericolo rispetto alla sicurezza, l'integrità e la disponibilità dei Sistemi del cliente.

(C) Impedire accesso, acquisizione, distruzione, perdita, cancellazione, divulgazione, alterazione o utilizzo non autorizzati o incidentali dei Dati del cliente o dei Sistemi del cliente.

(c) Uno o più dipendenti qualificati dell'Azienda vengono investiti della responsabilità di gestire il Programma di sicurezza delle informazioni dell'Azienda. Il programma è sostenuto e approvato dal top management dell'azienda per proteggere i Dati riservati dei clienti da perdite o uso improprio in relazione alle attività dell'Azienda previste dagli accordi contrattuali in vigore con i Clienti.

(d) Qualora la legge vigente impedisca il rispetto dei Requisiti di sicurezza o qualora la legge in vigore preveda requisiti più rigidi di quelli indicati nel presente Allegato, l'Azienda rispetterà la legge vigente.

(e) A richiesta, l'Azienda comunicherà al Cliente eventuali strutture di hosting terze condivise che ospitino i Dati del cliente e l'Azienda metterà in atto misure ragionevoli per contribuire a garantire che tali terze parti rispettino effettivamente i termini applicabili del presente Allegato.

(f) L'Azienda fornisce formazione su una gamma generale di argomenti relativi alla sicurezza delle informazioni fra cui, in modo non esaustivo, phishing e ingegneria sociale, fondamenti sulla sicurezza e protezione dei dati al Personale aziendale esistente con frequenza annuale e al nuovo Personale aziendale al momento dell'assunzione. Per il Personale aziendale che rientri nel perimetro degli Utenti privilegiati, l'azienda fornisce una formazione annuale obbligatoria, specifica per il ruolo, sulle politiche e gli standard di sicurezza aziendali.

## 4. CONTROLLO DEGLI ACCESSI

(a) L'Azienda consente l'accesso ai Dati o ai Sistemi dei clienti solo al Personale aziendale e alle terze parti che devono effettuare servizi previsti nel Contratto. Il Personale aziendale autorizzato e le terze

parti utilizzeranno i dati e i sistemi dei clienti sono nella misura necessaria per rispettare i propri obblighi derivanti dal Contratto e dal presente Allegato.

(b) L'Azienda applica il "Principio di minimo privilegio (PLP)" per garantire l'accesso unicamente alle informazioni legate all'attività del Cliente necessarie per effettuare una legittima funzione di business. L'Azienda adotta un metodo sicuro e affidabile per applicare controlli sulle autorizzazioni in modo da limitare gli accessi nel rispetto del PLP. La conformità al PLP richiede un processo che precluda immediatamente l'accesso da parte di Personale aziendale e terze parti che non richiedano più l'accesso per svolgere attività legate al Contratto (per es. un dipendente/appaltatore non più in servizio o destinato ad altre mansioni).

(c) L'Azienda dispone di un processo documentato per controlla gli ID degli utenti e altri identificatori per contribuire a garantire che siano unici fra gli utenti e non condivisi.

(d) L'Azienda seguirà le leggi vigenti, le misure degli standard di settore applicabili e le procedure di invecchiamento per limitare le opportunità di compromissione della sicurezza delle password e per l'autenticazione e l'autorizzazione degli utenti. L'Azienda non utilizzerà credenziali di identificazione condivise o generiche per accedere ai dati o ai sistemi dei clienti. Sono previste procedure relative alle password per garantire che:

(A) La password comprenda un minimo di otto (8) caratteri e

(B) comprenda almeno un carattere alfabetico, uno numerico e un carattere speciale.

(C) Inoltre, le password scadono dopo ogni novanta (90) giorni o meno

(D) e gli ID degli utenti sono disattivati dopo non oltre dieci (10) tentativi falliti di accesso.

(e) L'Azienda verifica l'identità degli utenti prima di ogni reset della password e gli account inattivi da 90 giorni vengono disattivati.

(f) Ove possibile, qualora una sessione sia inattiva da oltre quindici (15) minuti, all'utente viene richiesto di inserire nuovamente la password e di riattivare la sessione.

(g) Periodicamente, l'Azienda rivede e revoca i permessi di accesso degli utenti.

(h) L'Azienda fornisce e revoca credenziali di identificazione da essa gestiti tramite procedure di controllo tecniche e logiche documentate.

(i) L'autenticazione per accedere a risorse di rete, piattaforme, dispositivi, server, workstation e applicazioni aziendali non è concessa con password predefinite e, qualora disponibili, vengono utilizzati controlli di accesso basati sul ruolo.

(j) Se applicabile, tutti gli accessi ai dati e ai sistemi dei clienti avverrà tramite connessione sicura fra le località che ospitano i servizi dell'Azienda (incluso l'accesso tramite qualunque dei provider di servizi cloud dell'Azienda) e il Cliente.

## 5. PROTEZIONE DEI DATI SICURA

(a) L'Azienda memorizza i Dati riservati del cliente solo su dispositivi che soddisfino questi requisiti di sicurezza.

(b) L'Azienda utilizza misure standard di settore, fra cui la crittografia, per prevenire l'intercettazione o l'accesso alle Informazioni riservate che transitano attraverso le reti. Il transito attraverso la internet pubblica o altre reti accessibili dall'esterno richiede la crittografia.

(c) Le Informazioni riservate contenute su supporti cartacei o su supporti elettronici non crittografati vengono conservate in uno spazio controllato (per es. un ufficio personale dotato di porta) con una normale chiusura a chiave dopo l'orario di lavoro, oppure in contenitori chiusi a chiave (per es. un cassetto o un armadietto).

(d) L'utilizzo di Dati riservati del cliente in un ambiente non di produzione (di test o di sviluppo) è permesso solo quando sia approvato dal Cliente.

(e) L'Azienda gestisce procedure sicure per la distruzione dei dati, fra cui, in modo non esaustivo, l'uso di comandi di cancellazione sicuri, il degaussing o il "crypto-shredding", quando necessario. Le procedure aziendali seguono gli Standard di settore.

(f) Durante il trasporto fisico di supporti digitali che contengano Dati riservati del cliente, tali dati sono protetti mediante crittografia. Se approvato dal cliente, trasportare utilizzando un corriere qualificato, con tracking e in un contenitore fisicamente protetto. Il trasporto fisico di documenti cartacei o altri supporti fisici contenenti Dati riservati del cliente deve essere protetto dall'osservazione casuale delle informazioni ed effettuato utilizzando mezzi affidabili che prevedano il tracking.

(g) Se i Dati riservati del cliente sono archiviati o elaborati in un server o in un data center di proprietà dell'Azienda, tali strutture dovranno avere superato i controlli previsti nei presenti Requisiti per la sicurezza.

(h) L'Azienda è dotata di uno standard per la crittografia e la gestione delle chiavi che definisce gli standard di crittografia accettabili per essere utilizzati in tutti i sistemi e in tutti gli ambienti. Questo standard permette di affrontare problemi e offre chiarimenti in tema di crittografia identificando specifici requisiti che le risorse informative devono possedere:

(A) L'Azienda crittografa i Dati riservati del cliente a riposo, in transito e durante l'utilizzo mediante crittografia AES a un minimo di 128 bit e chiave di cifratura di 1024 bit di lunghezza.

(B) Prima del backup, tutti i Dati del cliente vengono crittografati o protetti in modo equivalente.

(C) L'Azienda utilizza metodi di crittografia standard di settore disponibili per il trasferimento dei dati di clienti mediante Internet.

## 6. SICUREZZA DEGLI ENDPOINT E DELLA RETE

(a) L'Azienda installa, configura e gestisce controlli di sicurezza al perimetro e nella rete, per prevenire l'accesso non autorizzato ai dati e/o ai sistemi dei clienti.

(b) L'Azienda gestisce e configura software di sicurezza degli endpoint su server, desktop, laptop, dispositivi mobili e dispositivi portatili di archiviazione digitale. La protezione degli endpoint può comprendere software di crittografia, sistemi di individuazione di incidenti, sistemi di prevenzione degli incidenti,, software anti-malware, secondo gli standard di settore. L'Azienda contribuirà a garantire che tali configurazioni generino allarmi all'Azienda e ai log accessibili dall'Azienda.

(c) L'Azienda implementa controlli secondo gli standard di settore (sia in frequenza che i n natura) in punti appropriati della rete aziendale per controllare l'ingresso e l'uscita di comunicazioni e dati ad ambienti contenenti Dati riservati del cliente.

(d) L'Azienda non bypasserà né tenterà di aggirare i controlli di sicurezza stabiliti dall'Azienda, compreso durante l'accesso esterno ai sistemi del Cliente.

(e) L'Azienda implementa e gestisce standard di sicurezza e di maggiore protezione per dispositivi di rete, inclusi, in modo non esaustivo, configurazioni di base, applicazione di patch, controllo degli accessi.

(f) L'Azienda segue procedure di gestione dei cambiamenti documentate.

(g) L'Azienda cambia le password predefinite dei server prima di porre in produzione dispositivi o sistemi.

(h) L'Azienda gestisce un log elettronico degli accessi e degli eventi per contribuire a garantire la conferma degli accessi e la protezione dei dati. I log sono protetti dall'accesso e dalla modifica non autorizzati, oltre che dalla distruzione accidentale o deliberata. I log vengono esaminati periodicamente.

(i) L'Azienda protegge in modo ragionevole le postazioni di lavoro dalle intrusioni implementando screen saver automatici, dispositivi di bloccaggio, schermi per la privacy e/o controlli simili.

## 7. GESTIONE DELLE APPLICAZIONI

(a) Indipendentemente dalla tecnologia di sviluppo, l'Azienda gestisce un processo di Ciclo di vita dello sviluppo del software (Software Development Life Cycle: SDLC) che include pratiche di codifica di sicurezza (per es. OWASP Top 10).

(b) Le attività di sviluppo, test e produzione delle applicazioni sono separate.

(c) L'accesso e l'archiviazione del codice sorgente delle applicazioni è limitato per supportare il Principio di minimo privilegio (Principle of Least Privilege: PLP) ed è gestito in un sistema dedicato (repository del codice sorgente). Il codice sorgente delle applicazioni è gestito mediante il controllo della versione.

(d) La documentazione sulle applicazioni è mantenuta aggiornata, conservata in forma accessibile e protetta da perdita o danneggiamento.

(e) Il software sviluppato internamente viene testato (incluso il test di regressioni), se applicabile, prima della distribuzione.

## 8. GESTIONE DEI RISCHI

(a) L'Azienda gestisce un programma per la valutazione dei rischi, che definisce ruoli e responsabilità per l'esecuzione della valutazione dei rischi e rispondere ai risultati. L'Azienda effettua annualmente una valutazione dei rischi per verificare il design dei controlli che proteggono le attività aziendali e l'information technology.

(b) L'Azienda gestisce un piano per il rimedio della valutazione dei rischi, che comprende l'uso del tracciamento dei rischi fino al completamento per misurare regolarmente l'avanzamento del rimedio rispetto alle date previste. Per l'accettazione di un rischio, il management dell'azienda fornirà un chiaro riconoscimento e una chiara descrizione del rischio. L'accettazione di un rischio comprende una giustificazione aziendale.

## 9. GESTIONE DELLE ATTIVITÀ

(a) I sistemi e i dispositivi aziendali coinvolti nel soddisfacimento di un Contratto sono gestiti e configurati in modo sicuro, conformemente a linee base e standard predefiniti. L'Azienda ha implementato software standard di settore per il rilevamento di virus/malware, periodicamente aggiornati.

(b) L'Azienda applica le patch di sicurezza e gli aggiornamenti di sistema al software, alle applicazioni, ai dispositivi e ai sistemi operativi gestiti dall'Azienda con tempistiche ragionevoli in base alla gravità della vulnerabilità, alla disponibilità delle patch e alla sensibilità dei dati coinvolti. Le patch saranno fornite al cliente in base alla loro disponibilità con il seguente programma, che definisce i limiti accettabili per il test e l'applicazione delle patch.

(i) L'Azienda conduce una periodica scansione delle vulnerabilità della sicurezza sui sistemi e le reti aziendali.

(ii) Annualmente, l'Azienda effettua un test di penetrazione di rete delle reti esterne.

(iii) L'Azienda identificherà, classificherà, documenterà e rimedierà alle vulnerabilità e ai rischi per i dati e i sistemi del cliente.

(iv) L'Azienda applicherà le patch di sicurezza e gli aggiornamenti di sistema al software, alle applicazioni, ai dispositivi e ai sistemi operativi gestiti dall'Azienda con tempistiche ragionevoli in base alla gravità della vulnerabilità, alla disponibilità delle patch e alla sensibilità dei dati coinvolti.

## 10. BUSINESS CONTINUITY E DISASTER RECOVERY

(a) L'Azienda gestisce un programma documentato di Business Continuity (BC). L'Azienda riesaminerà i propri piani di BC con frequenza almeno annuale.

## 11. GESTIONE E RISPOSTA AGLI INCIDENTI DI SICUREZZA

(a) Nell'ambito del proprio programma per la sicurezza delle informazioni, l'Azienda gestisce e aggiorna annualmente un piano documentato per la gestione e la risposta agli incidenti di sicurezza, nell'eventualità di una reale o sospetta compromissione della sicurezza.

(b) Il piano aziendale per la gestione e la risposta agli incidenti di sicurezza contiene procedure formali documentate che rispettano gli standard di settore e le leggi vigenti per affrontare l'indagine e la risposta a incidenti di sicurezza, incluse, in modo non esaustivo, le notifiche obbligatorie in caso di compromissione della privacy.

(c) L'Azienda collaborerà in modo ragionevole con il Cliente in ogni eventuale indagine relativa a uso o accesso fraudolento o non autorizzato ai dati o ai sistemi del cliente da parte di dipendenti dell'Azienda o di terze parti.

(d) Qualora l'Azienda scopra o venga informata di una violazione alla sicurezza che risulti in un accesso, acquisizione, divulgazione o utilizzo non autorizzati a dati o sistemi del Cliente o di una qualunque violazione dei presenti Requisiti per la sicurezza, l'Azienda comunicherà tali fatti al Cliente appena ragionevolmente possibile.

(e) L'Allegato sull'elaborazione dei dati descrive altre azioni che verranno intraprese dall'Azienda in caso di una violazione alla sicurezza.

## 12. SICUREZZA FISICA

L'Azienda utilizza le seguenti misure di sicurezza fisica ove Dati riservati del cliente siano conservati o accessibili.

(a) L'Azienda consentirà solo a individui autorizzati, con ragionevoli motivi aziendali, di accedere a zone e strutture aziendali dove tali Dati riservati del cliente siano conservati o accessibili.

(b) I sistemi per il controllo di accesso sono protetti da manomissione, aggiramento o distruzione e mantenuti costantemente funzionanti e vengono aggiornati o sostituiti qualora diventino compromessi o inefficaci.

(c) I controlli sulle strutture rispettano o superano gli standard di settore applicabili nel prevenire e rilevare eventuali compromissioni fisiche.

(d) L'Azienda rivede periodicamente la conformità dei controlli sulle strutture, per contribuire a garantirne l'allineamento con i requisiti di conformità e di sicurezza.

## 13. DIRITTO ALLA VERIFICA

(a) Non più di una volta per anno solare, su richiesta e a spese del Cliente, il Cliente può ragionevolmente verificare la conformità dell'Azienda con il presente Allegato. Tale verifica avrà luogo durante il normale orario di lavoro, a fronte di una richiesta scritta fatta pervenire all'Azienda almeno 30 giorni lavorativi prima. La verifica può avere luogo presso le strutture dell'Azienda o in modalità remota. Non più tardi di 2 settimane prima l'inizio della verifica, Azienda e Cliente concorderanno il perimetro e la durata della verifica.

(b) L'Azienda collaborerà ragionevolmente alla verifica del Cliente, fornendo al Cliente la documentazione a prova della conformità con il presente Allegato.

(c) A richiesta, l'Azienda discuterà i risultati della verifica con il Cliente e concorderà con il Cliente eventuali attività e tempistiche di rimedio, ove applicabile.

(d) A richiesta, ove applicabile, in sostituzione della verifica, l'Azienda fornirà al Cliente un questionario annuale sulla sicurezza (massimo una (1) richiesta per ogni periodo di dodici (12) mesi) per rispondere a specifiche domande sul programma per la sicurezza delle informazioni dell'Azienda.

**FINE DELL'ALLEGATO**