CLAUSULE CONTRATTUALI SULLA SICUREZZA DELLE INFORMAZIONI

Nota: Per qualsiasi necessità o chiarimento, il BUSINESS PARTNER può contattare infosec@altergon.it

Regolamento sulla Sicurezza delle Informazioni
Di seguito le clausole standard di information security che il BUSINESS PARTNER si impegna a rispettare. L'applicazione delle clausole considera il servizio fornito e il trattamento delle informazioni e risorse ALTERGON ITALIA.

INFORMATION SECURITY AND SECURITY BY DESIGN	
IL BUSINESS PARTNER:	
1.1	progetta, implementa, gestisce e mantiene servizi IT conformemente ad un approccio basato sul rischio e allineato agli standard di information security (ad esempio, ISO/IEC 27001, il Cybersecurity Framework del NIST) e alle normative applicabili.
1.2	garantisce che il servizio venga sviluppato e rilasciato su sistemi operativi supportati dal fornitore al momento dello sviluppo. Il Business Partner si impegna a garantire che, al momento dell'acquisizione, il servizio/prodotto non utilizzi sistemi operativi che hanno raggiunto la fine del loro supporto (End Of Life) e che nuovi sviluppi e rilasci siano su sistemi operativi supportati.
1.3	garantisce che la soluzione sia progettata, sviluppata e fornita in conformità con le migliori pratiche di sicurezza riconosciute. In particolare: • tecnologie, protocolli, librerie e funzionalità obsolete, deprecate o pubblicamente riconosciute come insicure non devono essere utilizzate. • le attività di sviluppo software devono essere conformi alle linee guida e agli standard riconosciuti dal settore, es. OWASP o ad altri standard internazionali applicabili. • i requisiti di sicurezza devono essere formalmente definiti, documentati e valutati durante le fasi di progettazione e pianificazione dei servizi e/o delle soluzioni. • principi di Secure-by-Default e sviluppo sicuro devono essere applicati durante tutto il ciclo di vita della soluzione, per minimizzare i rischi di sicurezza e ridurre la superficie di attacco.
1.4	garantisce che i dati sensibili ALTERGON ITALIA archiviati all'interno del sistema e trasmessi attraverso le reti siano protetti tramite crittografia. La crittografia deve essere implementata utilizzando algoritmi e standard crittografici ben noti e riconosciuti nel settore. L'uso di algoritmi di crittografia proprietari o non pubblici è severamente vietato.
1.5	garantisce che per la soluzione siano abilitate le funzionalità di logging ventiquattro (24) ore su ventiquattro, sette (7) giorni su sette. I registri devono essere conservati per un periodo appropriato, in conformità con i requisiti di sicurezza, le esigenze operative e le normative applicabili. I dati di log devono essere generati e mantenuti in un formato leggibile e standardizzato, esportabili e condivisibili con strumenti interni di monitoraggio e sicurezza (ad esempio, SIEM).

ACCESS MANAGEMENT	
IL BUSINESS PARTNER:	
2.1	garantisce che la soluzione offra integrazione nativa con Microsoft Entra ID o, almeno, con Active Directory, per supportare l'autenticazione in Single Sign-On (SSO). La soluzione deve sfruttare protocolli di autenticazione e autorizzazione standard del settore e garantire una gestione fluida dell'identità utente tra i sistemi integrati.
2.2	garantisce che, nel caso in cui l'integrazione con Microsoft Entra ID o Active Directory non sia tecnicamente fattibile, la soluzione IT debba implementare le seguenti misure minime di sicurezza: • l'uso di profili utente unici e personali per ogni utente autorizzato. • gestione e archiviazione sicure delle credenziali utente (ID utente e password), in conformità con le migliori pratiche del settore e gli standard di sicurezza applicabili.

CLAUSULE CONTRATTUALI SULLA SICUREZZA DELLE INFORMAZIONI

	• l'applicazione di una politica sulle password allineata agli standard di sicurezza riconosciuti dal settore, inclusi, ad esempio, una lunghezza minima della password di almeno otto (8) caratteri. • l'adozione dell'Autenticazione Multi-Factor (MFA) per rafforzare l'autenticazione degli utenti e ridurre il rischio di accessi non autorizzati.

VULNERABILITY AND PATCHING MANAGEMENT	
IL BUSINESS PARTNER:	
3.1	garantisce un processo strutturato di gestione delle vulnerabilità per garantire che le vulnerabilità vengano sistematicamente identificate, valutate, prioritizzate in base al rischio, rimosse tempestivamente e successivamente verificate per l'efficacia.
3.2	garantisce che le patch di sicurezza vengano applicate tempestivamente quando vengono identificate nuove vulnerabilità. Nei casi in cui una patch immediata non sia fattibile, devono essere implementate misure di mitigazione del rischio appropriate per proteggere il sistema e i suoi dati. Tutte le azioni devono essere svolte in conformità con le migliori pratiche del settore e gli standard di sicurezza pertinenti per minimizzare l'esposizione a potenziali minacce.

INCIDENT MANAGEMENT AND BUSINESS CONTINUITY	
IL BUSINESS PARTNER:	
4.1	informa immediatamente ALTERGON ITALIA, anche in ore extra-lavorative, di qualsiasi evento significativo di sicurezza informatica che coinvolga i servizi e/o le risorse correlate ad ALTERGON ITALIA, contattando: *infosec@altergon.it*
4.2	notifica a ALTERGON ITALIA senza indebito ritardo e in ogni caso entro 24 ore, dal momento in cui si viene a conoscenza di qualsiasi incidente di sicurezza, effettivo o sospetto che: • compromette la riservatezza, l'integrità o la disponibilità dei dati o dei sistemi. • potrebbe avere un impatto significativo sui servizi.

AUDITABILITY AND MONITORING	
ALTERGON ITALIA, IN ACCORDO CON IL BUSINESS PARTNER, PUÒ CONDURRE AUDIT REGOLARI PER VERIFICARE LA CONFORMITÀ ALLE CLAUSOLE SULLA SICUREZZA DELLE INFORMAZIONI.	
IL BUSINESS PARTNER:	
5.1	fornisce prove dell'efficace implementazione delle suddette misure di sicurezza tecniche su ragionevole richiesta da parte di ALTERGON, migliorando costantemente la propria postura di sicurezza in risposta alla continua evoluzione di minacce, vulnerabilità e pratiche del settore.
5.2	definisce un piano di rimedio per risolvere eventuali lacune identificate dall'ALTERGON ITALIA.
5.3	consentire l'accesso ai log che possano aiutare un'indagine forense in caso di compromessa, garantendo l'esportazione dei log su richiesta dell'ALTERGON ITALIA entro 5 (cinque) giorni.

INFORMATION SECURITY CONTRACTUAL CLAUSES

Note: For any need or clarification, the BUSINESS PARTNER can contact infosec@altergon.it

Information Security Regulations
Below the information security
The standard clauses that the BUSINESS PARTNER undertakes to respect. The application of the clauses is based on the service provided and treatment of ALTERGON ITALIA information and resources.

INFORMATION SECURITY AND SECURITY BY DESIGN	
THE BUSINESS PARTNER:	
1.1	designs, implements, operates, and maintains the IT services in accordance with a risk-based information security approach aligned with information security standards (e.g., ISO/IEC 27001, the NIST Cybersecurity Framework), and applicable cybersecurity regulations.
1.2	ensures that service is developed and released on operating systems that are supported by their vendors at the time of development. The Business Partner is committed to ensure that, at the time of acquisition, the service / product does not use operating systems that have reached the end of their support (End of Life) and that new developments and releases are on supported operating systems.
1.3	ensures that the solution is designed, developed, and delivered in accordance with recognized security best practices. In particular: • technologies, protocols, libraries, and functionalities that are outdated, deprecated, or publicly recognized as insecure must not be used. • software development activities shall comply with secure coding guidelines and industry-recognized standards, such as OWASP, or other applicable international security standards. • security requirements shall be formally defined, documented, and assessed during the design and planning phases of the services and/or solutions. • secure-by-default configurations and secure development principles shall be applied throughout the entire solution lifecycle, to minimize security risks and reduce attack surface.
1.4	ensures that ALTERGON ITALIA sensitive data stored within the system and transmitted across networks shall be protected exclusively through encryption. Encryption shall be implemented using well-known, industry-recognized cryptographic algorithms and standards; the use of proprietary or non-public encryption algorithms is strictly prohibited.
1.5	ensures that for the solution logging functionalities are enabled, twenty-four (24) hours a day, seven (7) days a week. Logs shall be retained for an appropriate period, in accordance with security requirements, operational needs, and applicable regulations. Log data shall be generated and maintained in a readable and standardized format and shall be exportable and shareable with internal monitoring and security tools (e.g., SIEM).

ACCESS MANAGEMENT	
THE BUSINESS PARTNER:	
2.1	ensures that the solution provides native integration with Microsoft Entra ID or, at a minimum, with an Active Directory, to support and enforce Single Sign-On (SSO) authentication. The solution must leverage industry-standard authentication and authorization protocols and ensure seamless user identity management across integrated systems.
2.2	ensures that, in case integration with Microsoft Entra ID or Active Directory is not technically feasible, the IT solution must implement the following minimum-security measures: • the use of unique and personal user profiles for each authorized user.

INFORMATION SECURITY CONTRACTUAL CLAUSES

	• secure management and storage of user credentials (user ID and password), in accordance with industry best practices and applicable security standards. • the enforcement of a password policy aligned with industry-recognized security standards, including, by way of example, a minimum password length of at least eight (8) characters. • the adoption of Multi-Factor Authentication (MFA) to strengthen user authentication and reduce the risk of unauthorized access.

VULNERABILITY AND PATCHING MANAGEMENT	
THE BUSINESS PARTNER:	
3.1	ensures a structured vulnerability management process to ensure that vulnerabilities are systematically identified, assessed, prioritized based on risk, remediated in a timely manner, and subsequently verified for effectiveness.
3.2	ensures that security patches are applied promptly when new vulnerabilities are identified. In cases where immediate patching is not feasible, appropriate risk mitigation measures must be implemented to protect the system and its data. All actions shall be performed in accordance with industry best practices and relevant security standards to minimize exposure to potential threats.

INCIDENT MANAGEMENT AND BUSINESS CONTINUITY	
THE BUSINESS PARTNER:	
4.1	immediately informs ALTERGON ITALIA, also in extra-working hours, of any significant information security event that involves the services and/or resources related to ALTERGON ITALIA by contacting *infosec@altergon.it*
4.2	notifies ALTERGON ITALIA without undue delay, and in any case within 24 hours, upon becoming aware of any actual or suspected information security incident that: - Compromises the confidentiality, integrity, or availability of Customer data or systems; or - Could materially impact the Services.

AUDITABILITY AND MONITORING	
ALTERGON ITALIA MAY CONDUCT REGULAR AUDITS TO VERIFY THE BUSINESS PARTNER COMPLIANCE WITH INFORMATION SECURITY CLAUSES.	
THE BUSINESS PARTNER:	
5.1	provides evidence of the effective implementation of the above technical security measures upon reasonable request by ALTERGON ITALAI, and must continuously improve the technical security posture of the IT services in response to evolving threats, vulnerabilities, and industry best practices.
5.2	define a remediation plan to remediate any findings identified by ALTERGON ITALIA.
5.3	enable access to logs that would assist in a forensic investigation in the event of a compromise, ensuring the export of logs at the request of ALTERGON ITALIA within 5 (five) days.