ALLEGATO 1 – CONFORMITÀ ALLA DIRETTIVA UE 2022/2555 - NETWORK AND INFORMATION SECURITY 2 (NIS2)

Gestione del Rischio di Sicurezza. Keliweb S.r.l. adotta misure tecniche e organizzative appropriate per gestire i rischi per la sicurezza dei sistemi informativi e delle reti, in conformità alla normativa applicabile in materia di sicurezza informatica, cybersicurezza e protezione dei dati personali (incluse, a titolo esemplificativo e non esaustivo: la Direttiva NIS2 (UE 2022/2555), il D. Lgs. 138/2024 di recepimento e i provvedimenti, determinazioni e atti regolatori dell'Agenzia per la Cybersicurezza Nazionale (ACN) adottati in attuazione della disciplina NIS2; il Regolamento (UE) 2016/679 (GDPR) e il D. Lgs. 196/2003 come modificato dal D. Lgs. 101/2018; nonché, per i servizi erogati a pubbliche amministrazioni, i provvedimenti, determinazioni e atti regolatori dell'ACN in materia di qualificazione dei fornitori di infrastrutture cloud per la PA). Tali misure includono valutazioni periodiche del rischio, politiche di sicurezza documentate e procedure di revisione continua.

Notifica degli Incidenti. In caso di incidente di sicurezza significativo, Keliweb S.r.l. si impegna a notificare le autorità competenti e, ove applicabile, gli interessati, nei termini e con le modalità previsti da tutta la normativa applicabile (incluse, a titolo meramente esemplificativo e non esaustivo: le disposizioni sulla notifica degli incidenti di cui al D. Lgs. 138/2024 e ai provvedimenti, determinazioni e atti regolatori dell'ACN adottati in attuazione della disciplina NIS2; gli obblighi di notifica delle violazioni dei dati personali ai sensi degli artt. 33 e 34 del GDPR; nonché, per i servizi erogati a pubbliche amministrazioni, le eventuali ulteriori prescrizioni previste dai provvedimenti, determinazioni e atti regolatori dell'ACN in materia di qualificazione dei fornitori di infrastrutture cloud per la PA). Il cliente verrà informato senza indebito ritardo qualora l'incidente possa impattare i suoi dati o servizi.

Sicurezza della Catena di Fornitura. Keliweb S.r.l. valuta e gestisce i rischi di sicurezza derivanti dalla catena di approvvigionamento, inclusi fornitori terzi e provider di servizi ICT, in conformità a tutta la normativa applicabile (incluse, a titolo esemplificativo e non esaustivo: il D. Lgs. 138/2024 e i provvedimenti, determinazioni e atti regolatori dell'ACN adottati in attuazione della disciplina NIS2; i requisiti di sicurezza del trattamento di cui all'art. 32 del GDPR; nonché, per i servizi erogati a pubbliche amministrazioni, i provvedimenti, determinazioni e atti regolatori dell'ACN in materia di qualificazione dei fornitori di infrastrutture cloud per la PA). I contratti con i subfornitori critici includeranno clausole di sicurezza coerenti con i predetti obblighi

normativi.

Continuità Operativa e Disaster Recovery. Keliweb S.r.l. mantiene piani documentati di continuità operativa e ripristino in caso di disastro (BCP/DRP), testati regolarmente, al fine di garantire la continuità nella fornitura del servizio anche in caso di incidenti gravi, in conformità a tutta la normativa applicabile in materia di resilienza operativa e sicurezza (incluse, a titolo esemplificativo e non esaustivo: il D. Lgs. 138/2024 e i provvedimenti, determinazioni e atti regolatori dell'ACN adottati in attuazione della disciplina NIS2; le misure di sicurezza organizzativa e tecnica di cui all'art. 32 del GDPR; nonché, per i servizi erogati a pubbliche amministrazioni, i provvedimenti, determinazioni e atti regolatori dell'ACN in materia di qualificazione dei fornitori di infrastrutture cloud per la PA).