



ALLEGATO 2.1 - Standard di sicurezza

I termini in maiuscolo non altrimenti definiti nel presente documento hanno il significato loro assegnato nel Capitolato Tecnico, nel Contratto e nel DPA.

1. Programma di sicurezza delle informazioni. AWS manterrà un programma di sicurezza delle informazioni progettato per (a) consentire al Cliente di proteggere i Contenuti del Cliente contro la perdita, l'accesso o la divulgazione accidentale o illegale, (b) identificare i rischi ragionevolmente prevedibili per la sicurezza e la disponibilità della Rete AWS e (c) ridurre al minimo i rischi di sicurezza fisica e logica per la Rete AWS, anche attraverso una regolare valutazione e verifica dei rischi. L'AWS designerà uno o più dipendenti per il coordinamento e la responsabilità del programma di sicurezza delle informazioni. Il programma di sicurezza delle informazioni dell'AWS includerà le seguenti misure:

1.1 Sicurezza logica.

1.1.1 Controlli di accesso. AWS renderà la Rete AWS accessibile solo al personale autorizzato e solo nella misura necessaria per mantenere e fornire i Servizi. L'AWS manterrà i controlli di accesso e le politiche per gestire le autorizzazioni per l'accesso alla Rete AWS da ogni connessione di rete e utente, anche attraverso l'uso di firewall o tecnologie funzionalmente equivalenti e controlli di autenticazione. AWS manterrà controlli di accesso progettati per (i) limitare l'accesso non autorizzato ai dati e (ii) segregare i dati di ciascun cliente da quelli di altri clienti.

1.1.2 Accesso limitato agli utenti. AWS (i) fornirà e limiterà l'accesso degli utenti alla Rete AWS in conformità ai principi di minimo privilegio basati sulle funzioni lavorative del personale, (ii) richiederà la revisione e l'approvazione prima di fornire l'accesso alla Rete AWS al di sopra dei principi di minimo privilegio, compresi gli account di amministratore, (iii) richiederà una revisione almeno trimestrale dei privilegi di accesso alla Rete AWS e, se necessario, revocherà i privilegi di accesso alla Rete AWS in modo tempestivo e (iv) richiederà l'autenticazione a due fattori per l'accesso alla Rete AWS da postazioni remote.

1.1.3 Valutazioni di vulnerabilità. AWS eseguirà regolarmente valutazioni esterne delle vulnerabilità e test di penetrazione della Rete AWS e indagherà sui problemi identificati, seguendone la risoluzione in



modo tempestivo.

1.1.4 Sicurezza delle applicazioni. Prima di lanciare pubblicamente nuovi Servizi o nuove funzionalità significative dei Servizi, AWS eseguirà revisioni della sicurezza delle applicazioni volte a identificare, ridurre e correggere i rischi per la sicurezza.

1.1.5 Gestione delle modifiche. AWS manterrà controlli progettati per registrare, autorizzare, testare, approvare e documentare le modifiche alle risorse di rete AWS esistenti e documenterà i dettagli delle modifiche all'interno dei suoi strumenti di gestione delle modifiche o di distribuzione. AWS testerà le modifiche in base ai propri standard di gestione delle modifiche prima della migrazione alla produzione. AWS manterrà processi progettati per rilevare le modifiche non autorizzate alla rete AWS e seguirà i problemi identificati fino alla loro risoluzione.

1.1.6 Integrità dei dati. AWS manterrà controlli progettati per garantire l'integrità dei dati durante la trasmissione, l'archiviazione e l'elaborazione all'interno della Rete AWS. AWS fornirà a Sogei la possibilità di eliminare i suoi contenuti dalla Rete AWS.

1.1.7 Continuità operativa e disaster recovery. AWS manterrà un programma formale di gestione del rischio progettato per supportare la continuità delle sue funzioni aziendali critiche ("Programma di continuità aziendale"). Il Programma di continuità aziendale comprende processi e procedure per l'identificazione, la risposta e il ripristino di eventi che potrebbero impedire o compromettere materialmente la fornitura dei Servizi da parte di AWS (un "Evento BCP"). Il Programma di continuità operativa prevede un approccio in tre fasi che AWS seguirà per gestire gli eventi BCP:

(i) **Fase di attivazione e notifica.** Non appena AWS identifica problemi che potrebbero portare a un evento BCP, AWS li segnalerà, li convaliderà e li esaminerà. Durante questa fase, AWS analizzerà la causa principale dell'evento BCP.

(ii) **Fase di ripristino.** AWS assegna ai team appropriati la responsabilità di adottare misure per ripristinare la normale funzionalità del sistema o stabilizzare i servizi interessati.

(iii) **Fase di ricostituzione.** La leadership di AWS esamina le azioni intraprese e conferma che lo sforzo di ripristino è completo e che le porzioni interessate dei servizi e della rete AWS sono state ripristinate.



Dopo tale conferma, AWS conduce un'analisi post mortem dell'evento BCP.

1.1.8 Gestione degli incidenti. AWS manterrà piani di azione correttiva e piani di risposta agli incidenti per rispondere a potenziali minacce alla sicurezza della Rete AWS. I piani di risposta agli incidenti AWS prevedono processi definiti per rilevare, attenuare, indagare e segnalare gli incidenti di sicurezza. I piani di risposta agli incidenti AWS comprendono la verifica degli incidenti, l'analisi degli attacchi, il contenimento, la raccolta dei dati e la risoluzione dei problemi. AWS manterrà un bollettino di sicurezza AWS (alla Data di entrata in vigore, <http://aws.amazon.com/security/security-bulletins/>) che pubblica e comunica le informazioni relative alla sicurezza che possono interessare i Servizi e fornisce indicazioni per ridurre i rischi identificati.

1.1.9 Dismissione dei supporti di archiviazione. AWS manterrà un processo di disattivazione dei supporti che viene condotto prima dello smaltimento finale dei supporti di archiviazione utilizzati per memorizzare i Contenuti del cliente. Prima dello smaltimento finale, i supporti di archiviazione utilizzati per memorizzare i Contenuti del cliente saranno degaussati, cancellati, epurati, distrutti fisicamente o altrimenti sanificati in conformità alle pratiche standard del settore volte a garantire che i Contenuti del cliente non possano essere recuperati dal tipo di supporto di archiviazione applicabile.

1.2 Sicurezza fisica.

1.2.1 Controlli di accesso. AWS (i) implementerà e manterrà salvaguardie fisiche progettate per impedire l'accesso fisico non autorizzato, il danneggiamento o l'interferenza alla Rete AWS, (ii) utilizzerà dispositivi di controllo appropriati per limitare l'accesso fisico alla Rete AWS al solo personale autorizzato che abbia una legittima necessità aziendale di tale accesso, (iii) monitorerà l'accesso fisico alla Rete AWS utilizzando sistemi di rilevamento delle intrusioni progettati per monitorare, rilevare e avvisare il personale appropriato di incidenti di sicurezza, (iv) registrerà e verificherà regolarmente l'accesso fisico alla Rete AWS e (v) effettuerà revisioni periodiche per convalidare l'aderenza a questi standard.

1.2.2 Disponibilità. AWS (i) implementerà sistemi ridondanti per la Rete AWS progettati per ridurre al minimo l'effetto di un malfunzionamento sulla Rete AWS, (ii) progetterà la Rete AWS per anticipare e tollerare i guasti hardware e (iii) implementerà processi automatizzati progettati per spostare il traffico di dati dei clienti dall'area interessata in caso di guasto hardware.



1.3 Dipendenti AWS.

1.3.1 Formazione sulla sicurezza dei dipendenti. AWS implementerà e manterrà programmi di formazione sulla sicurezza dei dipendenti in merito ai requisiti di sicurezza delle informazioni dell'AWS. I programmi di formazione sulla sicurezza saranno rivisti e aggiornati almeno annualmente.

1.3.2 Controlli sul passato. Laddove consentito dalla legge e nella misura in cui è disponibile presso le autorità governative applicabili, l'AWS richiederà che ogni dipendente si sottoponga a un'indagine sui precedenti personali che sia ragionevole e appropriata per la posizione del dipendente e il livello di accesso alla rete AWS.

2. Valutazione continua. L'AWS effettuerà revisioni periodiche del programma di sicurezza delle informazioni per la Rete AWS. L'AWS aggiornerà o modificherà il suo programma di sicurezza delle informazioni se necessario per rispondere ai nuovi rischi per la sicurezza e per trarre vantaggio dalle nuove tecnologie.

3. Notifica di eventi di sicurezza. Se l'AWS viene a conoscenza di una violazione delle misure di sicurezza descritte nei presenti Standard di sicurezza che ha comportato (a) l'accesso illegale ai Contenuti del cliente memorizzati nelle apparecchiature o nelle strutture dell'AWS, oppure (b) l'accesso non autorizzato a tali apparecchiature o strutture, laddove, in entrambi i casi, tale accesso comporti la perdita, la divulgazione o l'alterazione dei Contenuti del cliente (ciascuno dei quali è un "Evento di sicurezza"), l'AWS provvederà tempestivamente a (i) notificare l'Evento di sicurezza al cliente e (ii) adottare misure ragionevoli per mitigare gli effetti e ridurre al minimo i danni derivanti dall'Evento di sicurezza.