NORME DI SICUREZZA PER LA TUTELA DEL PATRIMONIO INFORMATIVO DELLE AZIENDE DEL GRUPPO ALMAVIVA E DEI DATI GESTITI DA QUESTE PER I PROPRI CLIENTI

Sommario

1.1 PREMESSA

1.1.1 Le norme contenute nel presente documento integrano le Condizioni Generali degli OdA (“**Norme di Sicurezza**”). I Termini con la maiuscola, non definiti nelle Norme di Sicurezza, hanno il significato loro attribuito nelle Condizioni Generali. Il Fornitore prende atto che le Norme di Sicurezza sono pubblicate sul sito internet di AlmavivA S.p.A. al seguente indirizzo www.almaviva.it/it_IT/Area_fornitori e sono periodicamente soggette a revisione.

1.1.2 Le Norme di Sicurezza definiscono i controlli e gli standard di sicurezza che il Fornitore si impegna a mantenere attivi ed efficienti per tutta la durata di un OdA in forza del quale si trovi ad accedere ai sistemi e/o trattare dati e informazioni delle Società e/o da queste gestite per i propri clienti.

1.1.3 Il Fornitore si impegna, per tutte le attività inerenti e riconducibili allo svolgimento dei Servizi, ad adottare le politiche aziendali - opportunamente formalizzate, divulgate e disponibili per la consultazione internamente alla Società - coerenti con i contenuti della normativa vigente nonché ai contenuti delle regole di sicurezza comunicate e di seguito rappresentato.

1.1.4 Il Fornitore deve provvedere al trattamento dei dati in accordo con i loro livelli di classificazione e di servizio indicati dalla Società.

1.1.5 Il Fornitore dà atto e riconosce che i dati delle architetture e delle configurazioni dei sistemi informativi della Società, delle misure di sicurezza apprestate da quest’ultima, oltre che – in ogni caso - i dati relativi alle vulnerabilità eventualmente riscontrate in occasione dell’esecuzione del Servizio sono informazioni riservate (anche ai sensi dell’art. 98 del Codice della Proprietà Intellettuale) e che dalla loro diffusione all’esterno può derivare un pregiudizio grave alla Società, fra l’altro, in termini di esposizioni ad attacchi dall’esterno o di danni all’immagine ed alla reputazione.

1.1.6 Il Fornitore è tenuto a garantire, ove presenti, il rispetto dei livelli di servizio contrattualmente stabiliti con la Società anche in casi di emergenza o di contesa delle risorse da parte di altri suoi clienti.

1.1.7 Il Fornitore riconosce la proprietà esclusiva dei dati, del software, della documentazione tecnica e normativa e delle risorse sia logiche che fisiche ICT della Società qualora essi vengano utilizzati o comunque resi disponibili per l'erogazione del Servizio.

1.1.8 Il Fornitore prende atto che la violazione degli obblighi in materia di sicurezza indicati nel Norme di Sicurezza costituisce causa di risoluzione di diritto dell’OdA ai sensi dell’art.1456 c.c. con diritto della Società al risarcimento dei danni (anche d’immagine e/o reputazionali).

1.1.9 La Società avrà il diritto di revocare al Fornitore l'autorizzazione di effettuare qualunque attività sugli asset della Società (compresi i dati).

1.1.10 Su richiesta della Società, il Fornitore si impegna a cancellare in qualunque momento i dati di cui è venuto in possesso, indipendentemente dalla conclusione del rapporto contrattuale ed a fornire, su richiesta, l'evidenza della cancellazione effettuata.

1.1.11 Il Fornitore si impegna a restituire gli asset della Società (compresi dati, licenze e apparati) nei tempi concordati ed in ogni caso entro 60 giorni dalla cessazione dell'OdA.

1.1.12 Il Fornitore si impegna ad applicare, in materia di protezione dei dati personali, il Regolamento UE 2016/679 - GDPR e, per i trattamenti di dati personali svolti per conto della Società e/o di titolari terzi, ad attenersi agli obblighi, istruzioni e misure di sicurezza tecniche ed organizzative di cui al relativo atto di nomina ex art. 28 di detto Regolamento.

1.2 REFERENTI PER LA SICUREZZA

1.2.1 Il Fornitore e la Società, ove previsto, comunicano reciprocamente i nominativi dei referenti cui è affidata la gestione degli aspetti di sicurezza delle informazioni compresi, ove applicabile, i dati personali ("**Referente per la Sicurezza**"), che di norma sono assegnati al Responsabile di Coordinamento.

1.2.2 La Società ed il Fornitore si impegnano a comunicare tempestivamente ogni variazione in proposito.

1.2.3 La Società ed il Fornitore, per il tramite dei Referenti della Sicurezza, ove nominati, o dei Responsabili di Coordinamento, definiscono, di comune accordo, le procedure di comunicazione, coordinamento e gestione in caso di incidenti di sicurezza informatica, che possano anche compromettere i livelli di servizio contrattualmente definiti. Nel caso di trattamento di dati personali la procedura e la tempistica per la segnalazione degli incidenti e delle violazioni sono indicate nell'atto di nomina ex art.28 del Regolamento UE 2016/679 - GDPR della Società nei confronti del Fornitore.

1.3 PERSONALE E ORGANIZZAZIONE DEL FORNITORE

1.3.1 In relazione al personale comunque coinvolto nell'esecuzione dell'OdA (ivi compresi collaboratori a qualsiasi titolo), il Fornitore si impegna, anche ai fini della sicurezza delle informazioni:

- a garantire che lo stesso abbia qualifiche adeguate per i compiti svolti;
- a curare che tale personale riceva la necessaria formazione al riguardo e adeguate informazioni sulle regole di cui al precedente paragrafo 1.1;
- ad attuare, nell'assegnazione delle mansioni, le opportune politiche di separazione dei compiti;
- ad attribuire compiti e responsabilità al proprio personale al fine di presidiare le principali minacce interne ed esterne;

- nei casi di cessazione del rapporto di lavoro o di variazione di incarico, a garantire – tramite processi formalizzati e sicuri – la comunicazione immediata dell'evento alla Società e la revoca immediata delle credenziali concesse al proprio personale e la restituzione degli strumenti assegnati per lo svolgimento delle attività inerenti alle prestazioni contrattuali, come pure di eventuali badge, chiavi e altri strumenti di accesso, identificazione e autenticazione.

1.3.2 Il Fornitore si impegna a collaborare con la Società al fine di assicurare il raccordo con i ruoli e le procedure definite all'interno della Società per il processo di analisi dei rischi e degli adempimenti in materia di protezione dei dati personali ex Regolamento UE 2016/679 – GDPR.

1.3.3 Il Fornitore si impegna a tenere:

- una lista dei luoghi in cui sono ospitati:
  - i dati,
  - i Servizi,
  - i data center utilizzati dal Fornitore per la fornitura del Servizio,
- un documento indicante la gestione degli accessi fisici e logici e il numero di addetti con accesso ai dati della Società, nonché ad aggiornare regolarmente tale documentazione, consegnandola alla Società, previa richiesta per iscritto da parte della Società.

1.3.4 Il Fornitore si impegna a (**i**) comunicare tempestivamente alla Società la necessità di spostamento delle risorse e dei dati (compresi i backup) da un sito (suo o di terze parti) ad un altro, prima ancora che lo spostamento sia effettuato, ed (**ii**) ad implementare nel nuovo sito le stesse misure di sicurezza del sito primario. Resta comunque inteso che lo spostamento delle risorse e dei dati da un sito (suo o di terze parti) ad un altro deve essere preventivamente autorizzato dalla Società. Restano salvi eventuali divieti/restrizioni allo spostamento delle risorse e dei dati eventualmente già previsti nell'OdA.

1.3.5 Il Fornitore garantisce che, in caso di sub-affidamento, anche solo di parte, dei Servizi e/o di attività ad essi inerenti (che dovrà essere, in ogni caso, autorizzato per iscritto dalla Società e monitorato secondo le modalità previste nell'OdA), tutte le disposizioni relative alla gestione dei dati contenute nelle Norme di Sicurezza (con particolare riferimento alla riservatezza, retention e cancellazione dei dati), audit e verifiche siano applicate da tutta la catena di fornitura. Resta inteso che in caso di sub-affidamento il Fornitore sarà in ogni caso tenuto alla costante verifica e monitoraggio dei subaffidatari e dovrà tenere indenne e manlevata la Società in caso di danni (anche di immagine e reputazionali) da detti sub-affidatari causati.

1.3.6 Il Fornitore si impegna a comunicare preventivamente alla Società la propria intenzione di effettuare mutamenti nell'organizzazione del Fornitore che possano incidere sul livello di integrità, disponibilità e riservatezza dei dati, per consentire, alla Società, le opportune valutazioni e verifiche, anche a mezzo di un audit.

1.3.7 Il Fornitore si impegna a non introdurre modifiche (tecnologiche, di organizzazione dei servizi e della catena dei sub affidamenti) che possano diminuire la sicurezza del Servizio.

1.4 SICUREZZA FISICA E LOGICA DEL FORNITORE

1.4.1 Il Fornitore si impegna ad utilizzare per tutti i propri servizi aziendali, inerenti o riconducibili allo svolgimento delle prestazioni contrattuali, misure di sicurezza per la gestione delle credenziali e dei privilegi d'accesso conformi alle best practice ed alle norme di legge di cui al precedente punto 1.1.12 e che prevedano almeno:

- utenze univoche e personali;
- gestione sicura delle credenziali di accesso con scadenza periodica e modifica obbligatoria al primo accesso, garanzia di non riutilizzabilità e storicizzazione nel tempo e controlli automatici di robustezza;
- criteri e politiche di assegnazione delle credenziali e dei privilegi d'acceso che garantiscano l'adozione del criterio della separazione dei compiti;
- criteri e politiche di assegnazione dei privilegi d'accesso che garantiscano privilegi negati se non esplicitamente concessi e garanzia del criterio di minimo privilegio concesso;
- strumenti e policy di custodia dei supporti e dati ricevuti che prevengano la perdita e l'accesso anche accidentali da terzi.

1.4.2 Il Fornitore garantisce l'applicazione di misure di sicurezza fisica (quali, a titolo esemplificativo, chiusura dei locali, "clean desk policy", custodia dei supporti consegnati) nelle aree inerenti o riconducibili al Servizio fornito (e nei collegamenti da e verso tali sedi).

1.4.3 La distruzione di dati/supporti al termine delle attività contrattualmente previste sarà effettuata rispettando i requisiti di sicurezza definiti al precedente 1.1.12, e/o eventualmente indicati in OdA e/o comunicati tempo per tempo dalla Società.

1.4.4 Il Fornitore si impegna ad implementare adeguati meccanismi di isolamento dei dati gestiti per conto della Società rispetto ai dati gestiti per conto di propri altri clienti a garanzia della loro riservatezza, disponibilità ed integrità.

1.4.5 Il Fornitore, su richiesta della Società, si impegna a inviare una descrizione delle modalità con cui, in esecuzione dell'OdA, intende erogare il Servizio e implementare e gestire le misure di sicurezza informatica, fisica ed organizzativa per la protezione degli asset della Società, atte a garantire un servizio conforme al livello di classificazione richiesto.

1.5 USO SICURO DEI SISTEMI DEL FORNITORE

1.5.1 Il Fornitore si impegna, a garantire, per quanto riguarda il perimetro di responsabilità di propria competenza, la gestione delle attività sottoelencate:

- security incident management, attraverso l'individuazione, il contenimento, la segnalazione, la notifica e l'analisi degli eventi e degli incidenti di sicurezza delle

informazioni, individuando una opportuna escalation list. In particolare, si impegna ad informare immediatamente la Società, anche in orario extralavorativo, di qualsiasi evento significativo occorso in relazione alla sicurezza delle informazioni inerenti al servizio oggetto dell'OdA, inviando un report dell'incidente;
- rispettare i tempi di risposta agli incidenti di sicurezza concordati come specificato nel precedente paragrafo 1.2.3;
- patch management di sicurezza eseguito con processi di aggiornamento controllati e tempi adeguati alla gravità delle vulnerabilità;
- antimalware management con aggiornamento periodico;
- change management nell'attuazione di processi autorizzativi per l'esecuzione dei cambiamenti;
- dismissione controllata degli asset con l'adozione di sistemi di cancellazione sicura delle informazioni dai supporti di memorizzazione;
- divieto di rilasciare comunicati (anche attraverso canali quali media, social media, regulators, etc.) che abbiano come oggetto eventuali incidenti di sicurezza informatica accorsi, senza prima concordare con la Società i contenuti e le tempistiche della comunicazione.

1.5.2 Il Fornitore deve garantire l'esecuzione di attività di Vulnerability Assessment e Penetration Test interne sulle infrastrutture con cadenza almeno semestrale sul perimetro di pertinenza dei servizi erogati alla Società.

1.6 BACK UP DEI DATI

1.6.1 Il Fornitore si impegna ad eseguire il backup periodico dei dati inerenti alle attività contrattualmente previste (ivi compresi i dati di configurazione degli apparati e dei sistemi), con modalità tali da garantire:
- la conservazione delle copie di backup in un luogo sicuro e a prova di incendio e di intrusione;
- il recovery dalle copie di backup e l'esecuzione di test di recovery dedicati con cadenza prefissata.

1.6.2 La Società avrà il diritto di accedere alle copie di backup effettuate dal Fornitore.

1.7 FILE SHARING

1.7.1 Laddove per lo svolgimento delle attività assegnate dalla Società si renda necessaria la condivisione di file, data base, codice software (file-sharing), il Fornitore si impegna ad utilizzare esclusivamente piattaforme di file-sharing autorizzate dalla Società stessa. È pertanto espressamente vietato utilizzare altre piattaforme per il salvataggio e la condivisione delle informazioni. La Società si riserva di compiere attività continuative di monitoraggio degli strumenti di file–sharing utilizzate dal Fornitore.

1.8 LOG MANAGEMENT

1.8.1 Il Fornitore si impegna ad eseguire in maniera sistematica e formalizzata, nel rispetto della legge:

- la gestione dei log applicativi per i software inerenti o riconducibili allo svolgimento delle prestazioni contrattuali;
- la gestione dei log per i sistemi e apparati inerenti o riconducibili al servizio oggetto del contratto. Gli "event records" generati dai sistemi di autenticazione dovranno contenere riferimenti allo "username" utilizzato, alla data e all'ora dell'evento ("timestamp"), una descrizione dell'evento (quali, a titolo esemplificativo, sistema di elaborazione o software utilizzato; se si tratti di un evento di log-in, di log-out, o di una condizione di errore; quale linea di comunicazione o dispositivo terminale sia stato utilizzato), l'identificazione del sistema sul quale lo "username" ha operato.

1.8.2 I risultati delle tracciature dovranno essere conservati con modalità sicure (accesso autenticato e contenuti non alterabili) e verificabili, che garantiscano leggibilità, integrità e attendibilità ed esibiti alla Società, dietro richiesta.

1.8.3 Il Fornitore assicura la piena ricostruzione degli accessi e delle modifiche effettuate sui dati, anche per finalità ispettive.

1.9 SVILUPPO E MANUTENZIONE SOFTWARE

1.9.1 Nel caso di attività di sviluppo o manutenzione software o che comunque comportino la scrittura/modifica di software utilizzato dalla Società, il Fornitore si impegna a utilizzare tecniche di sviluppo sicuro del software, che prevedano almeno l'implementazione della validazione dei dati in ingresso, controlli di validazione dell'elaborazione interna, controlli di validità dei messaggi e dell'output, l'utilizzo di best practice riferite allo specifico linguaggio di programmazione o ambiente che si utilizza per lo sviluppo. Per tutta la durata dell'OdA, il Fornitore si obbliga a rispettare le linee guida di codifica sicura del software elencate nel Progetto Open Web Application Security (OWASP) e dal CWE/SANS Top 25 vigenti. Il Fornitore si obbliga altresì a rispettare il documento " Linee guida per la realizzazione di applicazioni web sicure per i Fornitori" contenente le linee guida per lo sviluppo sicuro del software della Società che il Fornitore prende atto ed accetta; tali linee guida sono consultabili nell'area riservata nella vostra scheda sul Portale Fornitori al seguente indirizzo https://www.almaviva.it/it_IT/Area_fornitori o in alternativa consegnate dal Responsabile di Coordinamento della Società come indicato nell'OdA e sono periodicamente soggette a revisione.

1.9.2 Nei limiti in cui le attività di cui sopra avvengano su ambienti gestiti dal Fornitore, quest'ultimo è tenuto ad assicurare:

- la separazione logica tra l'ambiente di produzione e gli altri ambienti;

- che gli ambienti di sviluppo, test e produzione siano dedicati alla Società e separati, almeno logicamente, dagli ambienti di altri clienti del Fornitore, a garanzia della loro riservatezza ed integrità;
- il divieto di utilizzare piattaforme di condivisione e repository per il codice software (tipo GitHub) diverse da quelle indicate dalla Società;
- eseguire le attività di test in maniera tale da garantire la loro oggettività, verificabilità e ripetibilità;
- non utilizzare i dati di produzione di proprietà della Società per le attività di test se non opportunamente anonimizzati;
- realizzare una completa documentazione dei test effettuati in ambito sicurezza;
- l'accesso a dati di produzione va contenuto ai casi di effettiva e comprovata necessità (ad es. manutenzione "correttiva in emergenza"), limitato al tempo strettamente necessario e comunque specificamente e preventivamente concordato.

1.9.3 Il Fornitore deve garantire l'esecuzione di attività di analisi statica e dinamica del codice software sul perimetro di pertinenza dei servizi erogati alla Società, impegnandosi altresì a fornire alla Società il report contenente la attestazione dell'assenza di vulnerabilità di tipo critico nei tempi concordati con la Società.

1.10 CONNESSIONE AI SISTEMI GESTITI DALLA SOCIETÀ

1.10.1 Nel caso di attività che richiedano la connessione di apparecchiature del Fornitore alle reti, sistemi server, applicazioni gestiti dalla Società, il Fornitore (fermo in particolare il rispetto, in relazione a tali apparecchiature, di quanto previsto ai precedenti punti 1.1.4 e 1.1.5) si impegna a:

- utilizzare le modalità e seguire in maniera puntuale le istruzioni impartite dalla Società per effettuare tale connessione;
- utilizzare (ove predisposte dalla Società) unicamente le reti d'accesso dedicate;
- utilizzare tale connessione, come pure gli ID, le password ed in generale le "credenziali d'accesso" fornite, unicamente al fine dell'esecuzione delle attività strettamente inerenti alle attività contrattuali;
- utilizzare, ove applicabile, connessioni sicure (anche a mezzo di VPN o strumenti di crittografia) per le connessioni effettuate tramite reti aperte (quali, a titolo esemplificativo, internet, wifi).

1.10.2 Il Fornitore prende atto e accetta che la Società ha facoltà di monitorare gli accessi e l'utilizzo fatto della connessione, anche per ragioni di sicurezza o di regolarità e continuità operativa, e di chiedere informazioni sulle caratteristiche tecniche di tali apparecchiature.

1.11 CREDENZIALI O STRUMENTI DELLA SOCIETÀ

1.11.1 In tutti i casi in cui il Fornitore sia stato dotato di credenziali o di strumenti informatici o di identificazione e di accesso (quali, a titolo esemplificativo, badge, chiavi, smart card,

certificati digitali) necessari per l'accesso ai sistemi dalla Società stessa, il Fornitore - nel rispetto delle normative vigenti – deve:

- garantire la capacità e affidabilità del soggetto assegnatario in relazione all'incarico per il quale è richiesta l'assegnazione delle credenziali/strumenti;
- curare che tali credenziali/strumenti siano custodite/i con la massima cura e non siano in alcun modo rese disponibili a terzi e siano utilizzate solo per lo svolgimento delle prestazioni contrattualmente previste;
- curare che non ne siano fatte copie, salvo ove autorizzate dalla Società;
- assicurare che delle credenziali e strumenti sia fatto uso esclusivamente da parte dei soggetti assegnatari; in tutti i casi in cui – in conformità alle regole vigenti – venga effettuato un cambio di assegnatario, verrà sottoscritto un documento per attestare tale cambiamento;
- segnalarne tempestivamente alla Società l'eventuale perdita di possesso (anche momentanea) come pure ogni possibile violazione delle norme di cui sopra;
- segnalare alla Società ogni altro evento (quale, a titolo esemplificativo, cessazione del rapporto di lavoro; modifica delle mansioni) che determini il venir meno della necessità di disporre di tali credenziali o strumenti.

1.11.2 In tutti i casi in cui il Fornitore operi su sistemi o su procedure della Società che prevedano l'utilizzo di strumenti di multi-factor authentication (strong-authentication) che richiedano l'utilizzo di device mobili, il Fornitore è tenuto a dotare il proprio personale interessato di smartphone con caratteristiche compatibili con gli standard della Società e numerazione telefonica cellulare che consenta ricezione di SMS e/o traffico dati (ad es. Microsoft Authenticator) elementi abilitanti all'utilizzo degli strumenti di multi-factor authentication utilizzati dalla Società per controllare ed autorizzare gli accessi ai propri sistemi informatici. Il numero di telefono associato allo smartphone dovrà essere assegnato al lavoratore in via esclusiva. È responsabilità del Fornitore segnalare tempestivamente eventuali cambiamenti di assegnazione.

1.11.3 In tutti i casi in cui il Fornitore sia stato dotato di credenziali, personali e non cedibili a terzi, necessarie per l'accesso ai sistemi dalla Società stessa, funzionali ed utilizzate esclusivamente per lo svolgimento delle attività svolte per le Società Almaviva, attraverso personal computer e device mobili del Fornitore, l'utilizzo delle suddette credenziali deve ritenersi di esclusiva responsabilità del Fornitore stesso. Il Fornitore che utilizza le credenziali Almaviva assume, dunque, la responsabilità esclusiva dell'eventuale uso irregolare, illegittimo, non sicuro dei software installati su tali dispositivi e/o scaricati dalla rete della Società e/o dall'account della Società nonché dell'installazione, download ed uso di software non autorizzati per iscritto dal Responsabile di riferimento della Società. L'autorizzazione conterrà il nome del prodotto, il vendor, l'edizione, la versione e le modalità di download e installazione del software stesso. Si specifica che nella definizione di software deve ritenersi incluso anche l'utilizzo di qualsiasi fonts proprietario non esplicitamente autorizzato dalla Società, con particolare riferimento a quelli utilizzati per la produzione di contenuti distribuibili all'esterno dell'organizzazione aziendale. In generale, salvo quanto formalmente autorizzato per iscritto e consegnato dalla Società al Fornitore, questi

deve dotarsi autonomamente di tutta l'attrezzatura individuale di hardware e software necessaria all'espletamento delle attività svolte per la Società.

1.12 ATTIVITÀ RELATIVE ALL'HARDWARE – SERVIZI SISTEMISTICI E TLC

1.12.1 In caso di ritiro o sostituzione di apparecchiature informatiche rese disponibili dal Fornitore e utilizzate dalla Società e/o di memorie di qualunque tipo che possano contenere programmi per elaborare o dati della Società, tutti i dati contenuti nelle memorie sostituite dovranno essere cancellati in modo irreversibile a cura del Fornitore, previo inserimento dei dati sulla nuova apparecchiatura o su idoneo supporto, secondo le richieste della Società.

1.12.2 In tutte le attività di manutenzione, come pure nei servizi sistemistici e di gestione delle reti, dovranno essere prese - in coordinamento con la Società - misure per prevenire la perdita anche accidentale di dati, anche residenti su apparecchiature diverse da quelle sulle quali si esegue l'intervento.

1.13 AMMINISTRATORI DI SISTEMA EX PROVVEDIMENTO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI DEL 27/11/2008 E S.M.I.

1.13.1 Qualora l'eventuale trattamento di dati personali da parte del Fornitore dovesse comportare anche attività di amministrazione di sistemi secondo le previsioni di cui al Provvedimento del Garante per la protezione dei dati personali del 27/11/2008 e s.m.i., il Fornitore è tenuto ad applicare le prescrizioni di cui al detto Provvedimento e, in particolare, quelle di seguito specificate.

1.13.2 Il Fornitore è tenuto ad effettuare le necessarie verifiche preventive di affidabilità degli amministratori di sistema, nonché le verifiche periodiche, almeno annuali, sul loro operato previste dal citato Provvedimento, dandone conto su richiesta della Società.

1.13.3 Il Fornitore è tenuto a mantenere una lista aggiornata degli "amministratori di sistema" abilitati ad operare sui dati e/o sui sistemi della Società ed a comunicarne gli estremi su richiesta e/o secondo le periodicità concordate.

1.13.4 L'accesso al sistema informativo della Società da parte di personale con privilegi amministrativi prevede accesso con autenticazione a due fattori (multi-factor authentication) basata su device mobile, in accordo a quanto previsto al punto 1.10.2.

1.13.5 Il Fornitore deve raccogliere e conservare per almeno sei mesi, con criteri non alterabilità, i log di accesso degli amministratori ai sistemi secondo prescrizioni di cui al citato Provvedimento.

1.14 AUDIT E VERIFICHE

1.14.1 Il Fornitore deve effettuare regolare attività di auditing al fine di verificare l'efficacia dei propri presidi di sicurezza. Il Fornitore deve consentire alla Società la valutazione e la verifica indipendente del rispetto delle Norme di Sicurezza e delle eventuali ulteriori disposizioni concordate mettendo a disposizione, per esempio, una certificazione secondo gli standard di settore o report di audit.

1.14.2 Quanto sopra non pregiudica il diritto della Società di condurre audit sul Fornitore e/o a procedere a richieste di informazioni anche da parte dei propri revisori e delle autorità

e/o organi di vigilanza, sia in caso di incidente di sicurezza sia come parte di una verifica periodica del rispetto delle disposizioni normative e contrattuali.

1.14.3 Il Fornitore deve prestare l'opportuna collaborazione all'effettuazione dell'audit e comunque consentire che i soggetti indicati al comma precedente possano intervistare il proprio staff e possano accedere:

- a tutte le informazioni e i documenti relativi ai Servizi;
- ai sistemi, strumenti, network, ai database, ai piani di continuità operativa, e altre informazioni relative ai Servizi;
- alle strutture e i locali dove il Servizio viene erogato.

1.14.4 Il Fornitore si impegna, ove richiesto, a predisporre gli opportuni remediation plan per eliminare eventuali non conformità riscontrate nei tempi che saranno concordati con la Società.

1.14.5 Il Fornitore concede alla Società il diritto di visionare - su richiesta della stessa - i risultati dei test delle attività di Vulnerability Assessment e Penetration Test svolte internamente dal Fornitore stesso sul perimetro di pertinenza dei servizi erogati alla Società.