Linee guida per la Fornitrice sul trattamento dei dati e l'utilizzo di infrastrutture tecnologiche

Versione 2.1 del 05/03/2021

Unipol Gruppo S.p.A.

Sede Legale: via Stalingrado, 45 - 40128 Bologna (Italia) - unipol@pec.unipol.it - tel. +39 051 5076111 - fax +39 051 5076666
Capitale sociale i.v. Euro 3.365.292.408,03 - Registro delle Imprese di Bologna, C.F. 00284160371 - P. IVA 03740811207 - R.E.A. 160304
Capogruppo del Gruppo Assicurativo Unipol iscritto all'Albo delle società capogruppo al n. 046

www.unipol.it

Sommario

1 Premessa

Le presenti linee guida, inerenti il trattamento dei dati e l'utilizzo delle infrastrutture tecnologiche della Committente, costituiscono le regole che la Fornitrice (in tale definizione sono altresì comprese parti contrattuali quali il lavoratore autonomo o il libero professionista) è obbligata ad osservare ed a far osservare alle persone dalla medesima autorizzate al trattamento dei dati personali della Committente, nonché a garantirne il rispetto da parte dei suoi sub-fornitori al fine di adempiere alle obbligazioni previste nel Contratto, di cui il presente documento ne costituisce parte integrante.

Tali linee guida si applicano nei confronti della Fornitrice che opera sul sistema informatico o sui dati della Committente, direttamente o tramite proprie infrastrutture tecnologiche.

Le linee guida si articolano in funzione dei seguenti macro-scenari di collaborazione da parte della Fornitrice:

- Accesso al sistema informatico della Committente;
- Sviluppo e/o manutenzione del software da parte della Fornitrice per conto della Committente;
- Erogazione dei servizi da parte della Fornitrice tramite la propria infrastruttura tecnologica.

La Committente si riserva di modificare il presente documento al verificarsi di variazioni normative in materia di privacy e sicurezza oppure in caso di cambiamenti delle proprie infrastrutture tecnologiche o delle relative politiche di sicurezza.

2 Politica di sicurezza della Committente

La Committente ha definito e adottato una politica di sicurezza delle informazioni aziendali (cui le presenti linee guida si ispirano) finalizzata a garantire la salvaguardia del proprio patrimonio informativo nonché la resilienza dei sistemi informatici e dei servizi di trattamento, nell'osservanza dei seguenti principi in materia di protezione dei dati:

- **Riservatezza**, assicurando che i dati siano accessibili solo ai soggetti autorizzati, trattati esclusivamente nell'ambito dei processi correlati e che siano altresì rispettate le regole stabilite dalla Committente inerenti al divieto alla diffusione e ai vincoli sulla comunicazione;
- **Integrità**, impedendo modifiche non autorizzate dei dati durante il trattamento, l'archiviazione o la trasmissione, al fine di garantire l'autenticità e l'inalterabilità dei medesimi; tale principio si intende altresì esteso ai sistemi informatici nel suo complesso;
- **Disponibilità**, assicurando che gli utenti autorizzati abbiano accesso tempestivo ed affidabile alle informazioni;
- **Non ripudio**, assicurando che l'informazione non possa essere disconosciuta da chi l'ha prodotta.

Per tutelare il proprio sistema informatico e al fine di poter ricostruire eventuali incidenti informatici, con particolare riferimento all'eventualità che tali incidenti abbiano un impatto in termini di violazione dei dati personali con un rischio elevato per i diritti e le libertà delle persone, la Committente traccia (adottando specifici log) gli accessi effettuati sulle proprie infrastrutture tecnologiche, nel rispetto della vigente normativa in tema di protezione dei dati personali.

Il termine di conservazione dei suddetti log è di sei mesi dalla data di registrazione dell'accesso al sistema informatico.

3 Regole Generali per il trattamento dei dati personali e l'utilizzo di infrastrutture tecnologiche e di strumenti elettronici/telematici

La Fornitrice deve attenersi alle seguenti disposizioni di carattere generale:

- trattare i dati personali in modo lecito e secondo correttezza, astenendosi dall'accedere a dati non pertinenti e non necessari alle attività regolate dal Contratto, siano essi protetti o meno da misure di sicurezza finalizzate ad evitare accessi non autorizzati;
- mantenere la riservatezza sui dati personali di cui si viene a conoscenza o in possesso per le suddette attività, astenendosi dal comunicare dati a soggetti diversi da quelli indicati dalla Committente;
- trattare i dati affinché siano esatti, completi, aggiornati e non eccedenti rispetto agli scopi per i quali vengono elaborati;
- applicare le misure di sicurezza previste dalla Committente al fine di evitare rischi di distruzione o perdita di dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta dei dati stessi;
- non diffondere i dati trattati, rendendoli pubblici;
- accedere solo alle porzioni del Sistema Informatico della Committente strettamente necessarie a svolgere le attività regolate dal Contratto;
- non utilizzare gli strumenti elettronici e telematici in violazione di legge, non mettere a rischio la sicurezza del sistema informatico o del patrimonio informativo o dei beni della Committente e non arrecare pregiudizio - anche sotto il profilo del danno all'immagine - alla medesima o a terzi;
- non utilizzare gli strumenti di comunicazione per ledere l'onore, il decoro o la reputazione della Committente o di terzi;
- non utilizzare strumenti elettronici e telematici privati (non aziendali) non autorizzati dalla Committente per lo svolgimento delle attività previste;
- non turbare o alterare il funzionamento delle infrastrutture tecnologiche della Committente, nonché intervenire senza diritto sui dati non pertinenti l'oggetto del contratto;
- non utilizzare abusivamente, o condividere con altri, codici di accesso (es. utenza e password) o altri dispositivi (es. badge) che consentano di accedere, in modo logico o fisico, a infrastrutture tecnologiche della Committente protette da misure di sicurezza e non permettere od agevolare un indebito accesso alle medesime;
- prevenire la diffusione di programmi informatici "infetti" (virus o altri codici maligni), cioè programmi diretti a danneggiare o interrompere servizi di infrastrutture tecnologiche;
- non utilizzare strumenti software o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni o documenti;
- utilizzare le infrastrutture tecnologiche esclusivamente per lo svolgimento delle prestazioni oggetto del Contratto;
- in assenza di espressa autorizzazione da parte della Committente, non effettuare scambi o spostamenti di risorse hardware della medesima o di parti o accessori di esse tra diversi utenti o sedi;
- utilizzare unicamente le risorse di rete autorizzate e messe a disposizione dalla Committente per

memorizzare e condividere file e informazioni correlate con le attività previste dal Contratto;

- non accedere a risorse di rete della Committente per cui non si è ricevuta autorizzazione, anche se eventualmente prive di protezione da accessi non autorizzati, nonché ai documenti ivi presenti, se non pertinenti con le attività contrattuali;
- restituire, a seguito della cessazione del rapporto contrattuale eventuali strumenti informatici ed elettronici messi a disposizione dalla Committente.

4 Accesso al sistema informatico della Committente

Nel caso di accesso al sistema informatico della Committente, la Fornitrice è tenuta a garantire la sicurezza dei propri accessi al medesimo e degli strumenti informatici utilizzati (PC, laptop, ecc.) adottando politiche e misure di sicurezza conformi a quelle adottate dalla Committente, riepilogate più avanti.

Per l'accesso al sistema informatico della Committente occorre inoltre disporre di credenziali di autenticazione, costituite da un codice identificativo personale (user-id) e da una password, e il relativo profilo di autorizzazione forniti dalla Committente, su richiesta del referente contrattuale della stessa cui la Fornitrice fa riferimento.

4.1 Regole per l'utilizzo del codice identificativo personale

La richiesta del codice identificativo personale, nonché delle abilitazioni necessarie, deve essere effettuata in anticipo allo svolgimento delle attività, tramite la procedura in vigore presso la Committente.

Al termine delle prestazioni oggetto del Contratto, user-id e relative abilitazioni informatiche saranno revocate.

È altresì vietato:

- utilizzare il codice identificativo personale di altri utenti;
- accedere contemporaneamente al sistema da diverse postazioni fisiche di lavoro, utilizzando il medesimo codice identificativo personale;
- trascrivere e lasciare incustodite le credenziali di accesso.

4.2 Regole per l'utilizzo della password

La password:

- deve essere personale e segreta;
- deve essere modificata periodicamente (almeno ogni 90 giorni);
- deve essere complessa, composta da un minimo di 8 caratteri, possibilmente utilizzando contemporaneamente maiuscole, minuscole, numeri e caratteri speciali (ove il sistema lo consenta);
- la password iniziale deve essere cambiata al primo collegamento.

4.3 Personal Computer (PC)

La Fornitrice, in funzione degli accordi contrattuali, potrà operare attraverso PC propri o eventualmente forniti dalla Committente.

4.3.1 PC della Committente

Il PC ha una configurazione standard, cioè una configurazione iniziale di applicativi predefiniti e identici per tutti i PC della Committente.

Solo il personale preposto dalla Committente può intervenire a modificare tale configurazione nonché le componenti hardware/software della macchina, salvo specifiche eccezioni concordate e autorizzate.

La Fornitrice è responsabile del corretto utilizzo e della conservazione del PC.

Nel caso di cessazione del rapporto contrattuale, la Committente provvederà a far ritirare il PC, facendo altresì cancellare il contenuto del disco fisso senza la possibilità di recuperare quanto precedentemente memorizzato.

Alcune regole a cui attenersi per l'uso del PC:

- non mettere in condivisione con altri soggetti porzioni di disco del PC;
- al termine della giornata lavorativa spegnere il PC (compresi monitor e stampante), al fine di assicurare un importante risparmio energetico e di preservare nel tempo l'integrità delle apparecchiature, salvo specifiche comunicazioni della Committente;
- non installare software, né modificare o cancellare/disabilitare software standard; la Committente valuterà il software più adatto nonché la compatibilità con i propri standard e provvederà alla relativa installazione e licensing;
- Qualora sia stato assegnato un PC portatile, prestare la massima attenzione e cautela al fine di non incorrere nell'eventuale rischio di furto o smarrimento.

4.3.2 PC della Fornitrice

Il PC della Fornitrice deve essere sempre allineato all'ultimo livello di sicurezza (*patch*) disponibile sia per il sistema operativo installato, sia per i vari software di produttività personale (ad es. Office, Java, Flash, Acrobat Reader, ecc.).

È responsabilità della Fornitrice verificarne e assicurarne il corretto e costante aggiornamento.

In caso di utilizzo di PC portatile, oltre alle norme elencate e alle precauzioni logistiche normalmente consigliate per ridurre il rischio di furto, è necessario adottare misure specifiche (es. crittografia di file o di zone del disco) a protezione dei dati della Committente eventualmente memorizzati in via temporanea.

4.4 Blocco automatico e manuale della sessione

4.4.1 PC della Committente

La configurazione standard del PC della Committente prevede l'attivazione automatica del blocco della sessione (*screen saver* o salvaschermo con password) dopo 15 minuti di inattività della macchina.

4.4.2 PC della Fornitrice

Nel caso invece il PC sia della Fornitrice, si applicano regole di configurazione analoghe a quelle indicate per il PC della Committente.

In entrambi i casi, quando ci si allontana dalla postazione di lavoro, il blocco della sessione deve essere attivato immediatamente in modo manuale (*Ctrl-Alt-Canc* e blocca il computer).

4.5 Politica Antivirus

4.5.1 PC della Committente

La configurazione del PC prevede un programma che, attivato automaticamente all'avvio del sistema operativo, identifica, segnala e rimuove virus e malware.

L'antivirus presente sui PC viene mantenuto automaticamente aggiornato quando connesso alla rete della Committente; le scansioni complete dei computer sono pianificate e gestite a livello centrale.

È vietato alla Fornitrice:

- cancellare o rimuovere il software anti-virus dal PC;
- inibire la scansione automatica del disco fisso del PC;
- installare software aggiuntivo - in particolare ulteriori antivirus, personal firewall o qualsiasi altro software - che potrebbe interferire con l'antivirus ufficiale installato e rendere il PC lento o instabile.

4.5.2 PC della Fornitrice

È responsabilità della Fornitrice garantire analoga politica di sicurezza con l'obiettivo di proteggere i dati e le infrastrutture tecnologiche della Committente da rischi di intrusione di virus/malware, con riferimento altresì all'obbligo di proteggere la postazione di lavoro (portatile od eventuale desktop) mediante patching, antivirus e firewall sempre attivi e costantemente aggiornati.

A tal fine la Committente si riserva inoltre la possibilità di utilizzare i c.d. sistemi di "*network protection"* per inibire l'accesso di strumenti elettronici non conformi alle suddette policies.

4.6 Posta Elettronica

La Fornitrice è tenuta a utilizzare per lo svolgimento delle attività contrattualmente previste il proprio sistema di posta elettronica.

Non è ammesso l'utilizzo di caselle di posta personali private (non aziendali) non autorizzati dalla Committente.

In casi particolari la Fornitrice, qualora autorizzata dalla Committente, può utilizzare caselle di posta elettronica impersonali condivise messe a disposizione da quest'ultima (ad esempio *Box-progetto-portale@committente.it*), sia per trasmettere, sia per ricevere messaggi.

In questi casi, la Fornitrice è responsabile del corretto utilizzo della posta elettronica e deve attenersi alle seguenti regole:

- la posta elettronica deve essere utilizzata esclusivamente per gli adempimenti contrattuali;
- non inviare messaggi con allegati o link a siti considerati non pertinenti agli adempimenti contrattuali;
- non rispondere a messaggi di mittenti sconosciuti o dei quali non sia possibile verificare l'identità;
- non aprire gli allegati o attivare link di e-mail ricevute da sconosciuti o riguardanti un oggetto sospetto al fine di limitare il rischio di virus o altri codici maligni;
- non abilitare programmi o macro ricevuti tramite posta elettronica dall'esterno della rete della Committente;
- non inviare all'esterno della rete della Committente, tramite posta elettronica, le credenziali di autenticazione, o configurazioni della rete interna, o informazioni sui sistemi informatici, banche dati, reti e procedure, o altre informazioni accessibili all'interno della rete della Committente, con particolare riferimento a informazioni riservate o confidenziali di proprietà della medesima;
- non inviare o rispondere a messaggi diffamatori, offensivi, osceni, contenenti discriminazioni o facenti parte delle cosiddette "catene di S. Antonio";
- non comunicare l'indirizzo di posta elettronica della Committente per usi non correlati alle prestazioni contrattuali (al fine di prevenire il fenomeno dello *spamming*);
- non iscriversi a mailing list;
- non installare o utilizzare software ricevuto come allegato di posta elettronica;
- non eccedere nella quantità e dimensione dei file allegati ai messaggi;
- procedere sempre alla compressione degli allegati, verificando a priori che il destinatario sia in grado di decomprimerli;
- procedere, ove possibile e proporzionalmente alla criticità del dato, alla protezione con password (e possibilmente anche tramite compressione crittografata) di allegati contenenti dati riservati o dati personali con particolare riferimento alle categorie particolari, escludendo in ogni caso la comunicazione di categorie particolari di dati personali tramite posta elettronica qualora oggetto di tutela ad opera di specifica normativa (ad esempio, test genetici e HIV). La password utilizzata per la protezione deve essere comunicata tramite un canale o modalità (ad es. sms) differente dal messaggio e-mail che contiene l'allegato.

4.7 Altri strumenti elettronici/telematici della Committente

4.7.1 Internet

L'abilitazione all'accesso a Internet tramite l'infrastruttura della Committente è subordinata al rilascio della user-id e necessita di preventiva autorizzazione della Committente stessa.

Per la navigazione in Internet la Fornitrice, la quale è responsabile del corretto utilizzo, deve inoltre attenersi alle seguenti regole:

- evitare l'accesso a siti non strettamente correlati all'assolvimento degli adempimenti contrattuali;
- evitare il download di software o altro materiale digitale che potrebbe violare le normative vigenti per la protezione del diritto d'autore, di provenienza illecita o poco attendibile, o comunque non attinenti alle prestazioni oggetto del Contratto;
- non sottoscrivere abbonamenti a pagamento, partecipare a blog, forum, newsgroup, chat line o bacheche elettroniche, registrarsi a guest book o servizi simili;
- non utilizzare la rete Internet, né la rete della Committente nel suo complesso, per connettersi in remoto ad altri computer;
- non portare a conoscenza di terzi, tramite la rete, credenziali di autenticazione, o configurazioni della rete interna, o informazioni sui sistemi informatici, banche dati, reti e procedure, o altre informazioni accessibili all'interno della rete della Committente, con particolare riferimento ad informazioni riservate o confidenziali di proprietà della medesima;
- segnalare immediatamente alla Committente eventuali anomalie riscontrate;
- non utilizzare l'infrastruttura tecnologica della Committente per l'accesso ad Internet tramite dotazioni (portatili, tablet, smartphone, etc.) private (non aziendali);
- è vietato l'utilizzo di sistemi di trasferimento e scambio dati non autorizzati dalla Committente.

4.7.2 WI-FI

Non è permesso alla Fornitrice, salvo ove espressamente autorizzato dalla Committente in deroga, di accedere alla rete wi-fi della Committente medesima.

4.7.3 Chat e Instant Messaging

Non è permesso alla Fornitrice, salvo ove espressamente autorizzato dalla Committente in deroga, di utilizzare gli strumenti di chat o instant messaging della Committente medesima.

4.7.4 Accesso remoto alla rete e alla infrastruttura della Committente

L'eventuale accesso da remoto alla rete e alla infrastruttura della Committente da parte della Fornitrice è permesso solo tramite VPN o altro strumento specifico similare messo a disposizione dalla Committente stessa.
Nel caso in cui la Fornitrice debba utilizzare un accesso remoto VPN (singolo o "LAN-to-LAN") alla rete informatica della Committente, è necessaria la preventiva autorizzazione della Committente stessa.

Devono essere inoltre rispettate le seguenti regole:

- ogni abilitazione è nominativa;
- durante il collegamento in VPN di un PC deve essere impedito che altre macchine possano utilizzare il canale per raggiungere la rete della Committente.

4.7.5 Badge

La Committente può assegnare alla Fornitrice - qualora l'espletamento dei relativi adempimenti contrattuali lo richieda - badge temporanei, associati univocamente, agli esterni per l'ingresso alle sedi che prevedono accessi regolati da tornelli o porte automatiche o eventualmente a quelle aree particolari o a quelle infrastrutture tecnologiche protette da specifiche misure di sicurezza.

Di seguito le regole cui attenersi per l'utilizzo del badge, coerentemente con le politiche interne della Committente:

- custodire il badge in modo diligente affinché non sia mai utilizzato da altre persone;
- non cedere il badge ad altra persona;
- utilizzare il badge esclusivamente per lo scopo per il quale è stato assegnato (apertura dei varchi di ingresso/uscita);
- restituire il badge alla Committente alla scadenza o interruzione del Contratto.

4.7.6 Telefonia fissa e mobile

La Committente, qualora specifiche esigenze contrattuali lo richiedano, può assegnare un apparecchio telefonico, la cui configurazione standard (ivi comprese le misure di sicurezza già presenti), non deve essere mai alterata.
L'apparecchio telefonico deve essere utilizzato esclusivamente per svolgere le prestazioni contrattuali e restituito alla relativa scadenza o interruzione.

5 Sviluppo e / o manutenzione del software da parte della Fornitrice per conto della Committente

Le regole di seguito esposte devono essere applicate a tutti i contratti che prevedono lo sviluppo e/o la manutenzione del software (in ambienti di sviluppo e test).

Il software sviluppato (in particolare gli applicativi Web, APP, API e web service) deve essere realizzato seguendo best practice internazionali di sviluppo di codice sicuro, quali le OWASP (Open Web Application Security Project).
Il software deve essere inoltre sottoposto da parte della Fornitrice a verifiche di sicurezza applicativa (es. analisi statica SAST, e/o dinamica, DAST) e, ove necessario, a test di carico; è opportuno che gli esiti di tali verifiche siano condivisi con la Committente prima della consegna finale.

È facoltà della Committente eseguire ulteriori propri test di sicurezza applicativa per il software commissionato alla Fornitrice; qualora emergano vulnerabilità, la Fornitrice è tenuta ad apportare le modifiche necessarie alla messa in sicurezza, senza alcun aggravio economico per la Committente.

La Fornitrice è tenuta inoltre a garantire in modo particolare che:

- nel codice software sviluppato o in manutenzione non siano presenti dati personali o informazioni di carattere riservato (ad esempio credenziali di autenticazione o indirizzi IP interni);
- il codice software prodotto ex-novo oppure personalizzato per la Committente non sia in alcun modo utilizzato, divulgato o pubblicato fuori dal contesto indicato dalla medesima (ad esempio se esposto e/o condiviso sui forum o sui social network, su piattaforme di sviluppo open source, repository pubblici o simili), né dalle persone autorizzate dalla Fornitrice al trattamento dei dati personali della Committente, né dai propri sub-fornitori.

5.1 Ambiente di Sviluppo e Test presso la Committente

- Lo sviluppo e il test di un software applicativo o di sistema deve essere eseguito in ambienti diversi e separati da quello di Produzione;
- la Fornitrice è tenuta all'utilizzo dei repository di Configuration e Change Management della Committente,
- gli strumenti di *Change e Configuration Management* utilizzati dalla Committente gestiscono:
    - le autorizzazioni di accesso ai vari ambienti di Sviluppo, Test/Collaudo, Produzione (incluse le librerie del codice sorgente),
    - il versionamento del software nei diversi ambienti,
    - la tracciatura delle modifiche apportate al codice sorgente,
    - il passaggio degli elementi da un ambiente a un altro previa approvazione;
- il piano dei test deve comprendere:
    - unit test,
    - system test,
    - integration test,

    - test di non regressione,
    - test di certificazione utente,
    - test di performance (ove necessario),
    - test di sicurezza (ove necessario, ad es. analisi statica/dinamica, vulnerability assessment/penetration test);
- le registrazioni dei test eseguiti costituiscono evidenza delle attività effettuate e dei loro esiti;
- i passaggi in produzione avvengono con modalità codificate e tempi pianificati.

5.2 Ambiente di Sviluppo e Test presso la Fornitrice

Il requisito richiesto è quello di evitare ogni commistione tra ambienti diversi, a garanzia dell'integrità dei dati trattati; conseguentemente l'ambiente di test deve essere fisicamente e logicamente separato da un eventuale ambiente di produzione della Committente, della Fornitrice o di altri clienti della Fornitrice.

- È opportuno che il software venga gestito dalla Fornitrice con strumenti *Change e Configuration Management* propri che garantiscano:
    - le autorizzazioni di accesso ai vari ambienti di Sviluppo, Test/Collaudo, Produzione (incluse le librerie del codice sorgente),
    - il versionamento del software nei diversi ambienti,
    - la tracciatura delle modifiche apportate al codice sorgente,
    - il passaggio degli elementi da un ambiente a un altro previa approvazione.
- Per gli ambienti di sviluppo e test devono essere utilizzati dati non reali, oppure resi anonimi o mascherati, a meno di accordi specifici con la Committente.
- Il piano dei test deve comprendere:
    - unit test,
    - system test,
    - test di non regressione,
    - test di performance (ove necessario),
    - test di sicurezza (ove necessario)
- le registrazioni dei test eseguiti costituiscono evidenza delle attività effettuate e dei loro esiti;
- Il software deve essere quindi consegnato alla Committente per consentire l'esecuzione degli ulteriori test (es. test di integrazione, certificazione utente, e test di sicurezza/performance ove necessario) prima dell'effettivo passaggio in produzione.

6 Erogazione dei servizi da parte della Fornitrice tramite propria infrastruttura

Qualora la Fornitrice operi - presso locali e tramite infrastrutture proprie o di propri sub-fornitori (ad es. con soluzioni di outsourcing o cloud) – erogando servizi informatici che interessano dati della Committente, è tenuta ad applicare (nonché a garantire che anche i propri sub-fornitori adottino analoga condotta) politiche e misure di sicurezza conformi a best practice e standard internazionali (quali ad esempio ISO/IEC 270xx, NIST CSF, ecc.) e al Regolamento Europeo di Protezione dei Dati Personali 2016/679 (*GDPR*), nonché ogni altra istruzione specifica eventualmente impartita dalla Committente e, in quanto applicabili, le presenti linee guida.

6.1 Sicurezza fisica e ambientale

La sicurezza fisica e ambientale inerente edifici e locali dai quali la Fornitrice eroga le prestazioni oggetto del Contratto, che presuppone la tutela dei dati della Committente, deve essere garantita da regole inerenti controlli, modalità e responsabilità per la gestione di tali aree, con particolare riferimento alla sicurezza degli accessi.

Di seguito le principali regole cui la Fornitrice deve attenersi:

- i punti di accesso agli edifici devono essere presidiati, tutti gli accessi e le uscite devono essere tracciati;
- il perimetro esterno e gli edifici della Fornitrice devono essere protetti da sistemi antintrusione e, se del caso, anche da sistemi di videosorveglianza;
- le porte che non sono adibite all'entrata negli edifici (in particolare quelle adibite a mera uscita di sicurezza), devono essere dotate di sistema di allarme;
- per gli accessi al Data Center deve essere prevista autorizzazione specifica;
- tutti gli accessi al Data Center devono essere tracciati;
- il personale esterno deve essere accompagnato per tutto il tempo da un referente interno della Fornitrice;
- per i suddetti locali devono essere predisposte misure di protezione attive e passive di rilevazione dei tentativi di accesso non autorizzati, nonché barriere fisiche e protezione dei sistemi;
- al fine di mitigare minacce di tipo ambientale quali incendi, allagamenti, terremoti o altre forme di eventi naturali dannosi o accidentali/volontari, devono essere adottate tutte le idonee contromisure, quali ad esempio: sistemi antincendio, antiallagamento, condizionamento, UPS e generatori elettrogeni, monitoraggio ambientale, ecc.;
- i sistemi di elaborazione e gli apparati di telecomunicazione devono essere posizionati in modo da mitigare i rischi da minacce ambientali e accessi non autorizzati.

6.2 Accessi Logici

Gli accessi logici alle informazioni devono essere autorizzati e monitorati. La Fornitrice deve autorizzare gli accessi agli ambienti contenenti i dati della Committente in relazione ai principi di "*need to know*", del "*least privilege*" e della separazione dei ruoli e compiti, assegnando in modo univoco i diritti di accesso ad ogni user account e garantendo a ciascuno utenze personali.

L’accesso ai dati deve essere tracciato e, per quanto tecnicamente possibile in relazione alle dimensioni e all’attività svolta dalla Fornitrice, deve conformarsi alle politiche di sicurezza adottate dalla Committente.

Ogni utente deve essere dotato di credenziali di autenticazione personali (username e password), sottoposto a un sistema di autorizzazione.

L’accesso al sistema informatico della Fornitrice deve essere consentito solo agli utenti autorizzati e con strumenti configurati per lo svolgimento delle attività previste; eventuali eccezioni devono essere autorizzate e tracciate.

Specifica attenzione deve essere prestata all’accesso a categorie particolari di dati personali.

Analoghe modalità devono essere adottate anche per l’accesso ai sistemi operativi e agli apparati di rete.

La Fornitrice garantisce che l'accesso da remoto (da reti pubbliche o comunque *non trusted*) agli ambienti che trattano dati della Committente deve essere protetto mediante almeno soluzioni di autenticazione con username, password e canale crittografato.

La Fornitrice deve mantenere un registro aggiornato delle utenze privilegiate (in particolare degli amministratori di sistema) abilitate a operare su dati e sistemi.

Le utenze degli amministratori devono essere personali e univoche, e utilizzare sistemi di autenticazione forte (es. OTP, certificati digitali, ecc.); in caso non siano presenti tali sistemi, la password deve avere criteri di robustezza, sufficiente lunghezza (es. almeno 14 caratteri) ed essere cambiata almeno ogni 90 giorni.

6.3 Gestione dei Sistemi e dell’Infrastruttura

La Fornitrice deve garantire:

- Una figura di riferimento per le tematiche di Sicurezza delle Informazioni;
- L’analisi e l’adeguata copertura dei rischi connessi alla sicurezza e protezione del dato, che prenda in esame anche la filiera di fornitura e sub-fornitura ICT, i sistemi tecnologici, l'elaborazione, la gestione, l’archiviazione, la trasmissione delle informazioni, gli eventi e gli incidenti di sicurezza;
- l’adozione delle misure di sicurezza secondo le best practice e gli standard internazionali (es. ISO/IEC 270xx, NIST CSF, ecc.);
- l’isolamento dei dati personali della Committente rispetto a quelli di altri Titolari in ambienti multi-tenant;
- la possibilità di adottare la crittografia dei canali di comunicazione (dati in transito) e dei dati a riposo, proporzionalmente alla criticità del dato trattato o secondo accordi stabiliti;
- la tracciatura degli accessi e operazioni ai propri sistemi, nel rispetto dei termini di conservazione e coerentemente con le normative vigenti; le informazioni contenute nei log devono essere protette contro la modifica e l’accesso non autorizzato.

La Fornitrice deve inoltre garantire un costante aggiornamento (*patching*) e irrobustimento (*hardening*) del software e delle configurazioni dei propri sistemi informatici, con cui eroga i servizi alla Committente, nonché effettuare periodicamente attività documentate di verifica dei livelli di sicurezza (es. sessioni di *Vulnerability Assessment e/o Penetration Test, analisi dei rischi IT e di adeguatezza delle misure di sicurezza)*, di cui dare evidenza alla Committente quando richiesto.

I sistemi, le applicazioni e i dati gestiti dalla Fornitrice devono essere protetti contro il rischio di intrusione e l'azione di programmi maligni mediante l'attivazione di idonei strumenti elettronici automatici (es. antivirus, antispam) costantemente aggiornati con periodicità definita.

L'ambiente e i dati di produzione della Committente devono essere fisicamente e logicamente separati da quelli di sviluppo e test.

La Fornitrice mette in atto adeguate procedure o prassi atte a garantire la disponibilità dei dati del Committente secondo quanto concordato, in particolare:

- prevede procedure di *backup* e *restore* dei dati con frequenza di salvataggio dei dati adeguata alle esigenze della Committente.
- Effettua periodicamente prove di ripristino (*restore*) dei dati, in modo da verificare l'utilizzabilità delle copie e del corretto funzionamento delle procedure.
- I dati archiviati sono tutelati da violazioni della riservatezza delle informazioni, mediante adeguata protezione di mascheramento o crittografia.
- L'eventuale copia fisica dei dati su supporti removibili è conservata adeguatamente (es. in altra sede) a garanzia dell'integrità e della riservatezza.

La Fornitrice si impegna nel ridurre al minimo il numero di archivi di dati del Committente (database, file, copie, archivi), evitando inutili duplicazioni.

Sono adottati opportuni sistemi e procedure per il monitoraggio e controllo dalla capacity e delle performance per assicurare le prestazioni del servizio erogato secondo gli SLA concordati.

Le modifiche infrastrutturali e applicative in produzione sono documentate, sottoposte a test preventivi e a workflow autorizzativi.

6.4 Gestione degli strumenti elettronici/telematici

La Fornitrice deve garantire che le politiche per la gestione dei propri server, postazioni di lavoro e altri strumenti elettronici/telematici utilizzati per il trattamento dei dati oggetto del Contratto, siano conformi a quelle adottate dalla Committente.
La Fornitrice inoltre deve proteggere i supporti (rimovibili e non rimovibili), contenenti dati della Committente, contro l'accesso non autorizzato attraverso adeguate misure di sicurezza fisica e logica (es. crittografia hard disk dei laptop, sistemi Mobile Device Management per smartphone/tablet, procedure di cancellazione sicura prima della dismissione).

6.5 Gestione della Rete

Le soluzioni adottate per la protezione delle reti di comunicazioni sono finalizzate a tutelare la riservatezza e la sicurezza delle informazioni, anche, ove necessario, mediante l'uso di crittografia tramite protocolli di rete sicuri.

La rete di telecomunicazioni della Fornitrice deve essere configurata in modo da presentare adeguati livelli di segregazione e devono essere impiegate componenti che offrano alternative di instradamento in caso di guasto, al fine di evitare singoli punti di debolezza.

Ai segmenti di rete, su cui opera la porzione del sistema informatico della Committente, si devono poter collegare esclusivamente sistemi riconosciuti; tali sistemi devono essere preventivamente identificati e registrati.

Eventuali collegamenti da remoto devono essere tracciati e attribuiti all'utente remoto registrato.

6.6 Gestione delle anomalie, degli incidenti e della continuità del servizio

La Fornitrice deve registrare tutti gli incidenti di sicurezza osservati o sospetti.

Ogni incidente di sicurezza deve essere valutato e gestito fino alla sua chiusura, eventualmente, attuando tutte le azioni correttive e di miglioramento necessarie a evitare che si ripeta.

I report degli incidenti, le analisi e le relative azioni correttive, preventive e di miglioramento, nonché i risultati delle verifiche di efficacia delle azioni pianificate, devono essere portati all'attenzione della Committente se hanno impatto sui sistemi, applicazioni e dati della medesima.

In caso di incidente di sicurezza con impatti su disponibilità, integrità e riservatezza, con particolare riferimento alla violazione dei dati personali, la Fornitrice ne deve fornire immediata comunicazione alla Committente secondo i termini ed utilizzando i contatti indicati nel Contratto stipulato tra le Parti.

In conformità alle leggi vigenti, con particolare riferimento alla normativa per la protezione dei dati personali, la Fornitrice, nell'ambito della risoluzione degli eventi di sicurezza, deve provvedere a raccogliere e conservare gli elementi probatori utili ad accertare le cause dell'incidente di sicurezza, anche al fine, se del caso, della difesa dei diritti in sede giudiziaria.

Le procedure di backup e di ripristino della Fornitrice su dati e software devono poter assicurare che gli stessi possano essere recuperati tempestivamente in caso di necessità (es. malfunzionamento, disastro).

La Fornitrice deve inoltre garantire un piano di *Business Continuity,* comprensivo di un piano di *Disaster Recovery* in conformità alle cogenze di settore, proporzionalmente alla criticità dei dati trattati per conto della Committente o secondo accordi stabiliti con la stessa.

Tali piani devono descrivere tutte le azioni necessarie ad assicurare il rispetto dei livelli di servizio contrattualmente previsti ed essere verificati almeno una volta l'anno.

La Fornitrice deve dare evidenza alla Committente, quando richiesto dalla medesima, di tali piani e dei relativi test eseguiti.

7 Trattamenti svolti mediante supporti cartacei

Il trattamento di documenti cartacei può avvenire presso i locali della Committente o presso quelli della Fornitrice.

Di seguito le regole generali nel caso di trattamento di dati personali mediante supporti cartacei, cui la Fornitrice deve attenersi al fine di garantire la protezione dei dati personali conservati o comunque oggetto di trattamento:

- garantire la riservatezza;
- fare uso di armadi, cassettiere e altri mobili muniti di serratura, siano essi interni o esterni all'ufficio (corridoi, locali comuni, archivi);
- tenere conto delle esigenze di sicurezza al fine di prevenire incendi o evitare altre cause di distruzione di dati;
- prestare particolare attenzione al trattamento e conservazione delle categorie particolari d dati personali (quali ad esempio quelli di carattere sanitario) o relativi a condanne penali e reati, anche in caso di abbandono temporaneo della propria postazione di lavoro;
- al termine dell'attività giornaliera riporre negli armadi chiusi a chiave i documenti contenenti dati personali;
- inserire nelle macchine distruggi-documenti (ove previste) tutto il materiale cartaceo eliminato contenente dati personali (lettere, note, stampe, documenti, etc.);
- utilizzare i cestini presenti in ufficio esclusivamente per trasferirvi carte da lavoro non contenenti dati personali;
- prestare attenzione alle fotocopiatrici e alle stampanti: se collocate nei corridoi o comunque in luoghi non presidiati, è importante ritirare contestualmente le stampe evitando di lasciarle incustodite;
- prestare attenzione che tutti i documenti siano resi indecifrabili prima del loro invio al macero;
- in caso di violazione dei dati personali, la Fornitrice ne deve fornire immediata comunicazione alla Committente secondo i termini ed utilizzando i contatti indicati nel Contratto stipulato tra le Parti.

Nel caso di trattamento di documentazione cartacea presso la Fornitrice, la medesima deve inoltre attenersi alle seguenti regole:

- i documenti conservati negli arredi o armadi a parete, muniti di serratura e chiusi a chiave, ubicati all'interno degli uffici o nei corridoi, devono essere accessibili esclusivamente al personale autorizzato, che di norma si limita agli addetti dell'ufficio che ne hanno competenza;
- impedire l'accesso da parte di terzi estranei, prestando particolare attenzione nell'eventualità di ricevimento del pubblico;
- nel caso di locali adibiti a esclusivo uso di archivio interno, i medesimi devono essere accessibili solo alle persone autorizzate, devono essere sempre chiusi a chiave al termine dell'orario di lavoro e devono essere sottoposti a controlli per verificare la corretta custodia dei documenti

riposti;

- nel caso la Fornitrice abbia affidato ad ulteriori soggetti l'incarico di gestire e conservare presso le rispettive strutture alcune tipologie di documenti, la medesima deve sottoscrivere specifici contratti definiti nell'osservanza della normativa privacy, al fine di garantirne la riservatezza e sicurezza.