

Art. 1 Premessa

Le presenti Condizioni Generali di fornitura di servizi Cloud del CSI-Piemonte (di seguito, Condizioni Generali) regolano le condizioni d'utilizzo della piattaforma Cloud offerta ai fornitori del Consorzio e funzionale all'erogazione di beni o servizi o soluzioni applicative a favore del CSI stesso o dei suoi Clienti e regolati da specifico e distinto accordo negoziale, cui le presenti condizioni costituiscono eventualmente allegato.

Le presenti Condizioni Generali - rese disponibili anche sul Service Portal - rispettano i principi sanciti in questi ultimi anni dalle Autorità Europee per garantire una maggiore tutela del Cliente finale, un elevato livello di protezione e sicurezza dei suoi dati e in generale la massima chiarezza e trasparenza delle clausole contrattuali.

In particolare, si fa riferimento ai principi contenuti nel Parere n. 05/2012 del 1.7.2012 (WP196) del Gruppo delle Autorità per la privacy europee (Gruppo di Lavoro Articolo 29), nel Parere del 16.11.2012 del Garante Europeo della Protezione dei dati sulla Comunicazione della Commissione Europea suindicata, nel documento esplicativo delle BCR (Regole Vincolanti d'Impresa) del 19.3.2013 e nelle clausole contrattuali tipo contenute nel Final Report di novembre 2013 per gli accordi di servizi cloud e soprattutto nel recente Regolamento Europeo Generale in materia di protezione dei dati personali – GDPR 2016/679, nelle “Guidelines on the use of cloud computing services by the European institutions and bodies”, pubblicate dall'EDPS il 16 Marzo 2018, nella direttiva europea NIS (UE) 2016/1148 per quanto riguarda la sicurezza di reti e dei sistemi informativi attuata con D.Lgs. 65/2018.

Inoltre, il CSI Piemonte è certificato ISO 27001 per i servizi di Facility Management e applica i controlli previsti dalla norma ISO/IEC 27017 e 27018 nell'analisi, nella predisposizione e nella gestione dei propri servizi cloud, in qualità di Cloud Provider.

Art. 2 Definizioni

Agli effetti delle presenti Condizioni Generali e dei documenti allegati si intende per:

- **"CSI"**: il CSI Piemonte con sede in Torino, corso Unione Sovietica 216, 10134, Torino ;
- **"Cliente finale"**: l'Ente che ha richiesto al CSI l'attivazione di uno o più soluzioni applicative e/o beni/servizi da erogarsi attraverso (o anche attraverso) la piattaforma cloud;
- **"Utente"**: la persona fisica individuata da CSI e/o dal Cliente come incaricato ed autorizzato ad utilizzare uno o più soluzioni applicative per conto del CSI e/o Cliente stesso, in quanto appartenente alla rispettiva organizzazione;
- **"Soluzione Applicativa"**: è l'insieme delle funzionalità richieste dal CSI o dal Cliente affinché i propri Utenti possano svolgere le proprie attività;
- **"Fornitore Terzo"**: soggetto con cui CSI ha sottoscritto – o in corso di sottoscrizione - un Contratto funzionale all'acquisizione di beni/servizi/Soluzioni applicative nell'interesse proprio e/o dei propri Clienti, le cui condizioni prevedono in via obbligatoria o facoltativa (cui il Fornitore ha nel caso ritenuto di aderire) l'uso dei servizi Cloud offerti dal CSI, nei termini precisati dall'accordo stesso;
- **"Referente tecnico"**: persona fisica del Fornitore Terzo individuata da quest'ultimo come punto di contatto a cui il CSI potrà fornire le informazioni necessarie alla finalizzazione del Servizio, avrà accesso al “Service Portal” con ruolo amministrativo come di seguito definito,
- **"Incaricati Autorizzati"**: elenco di persone individuate dal Fornitore Terzo ad accedere ai servizi Cloud;

- **"Contratto"**: l'accordo stipulato o da stipularsi fra CSI ed il Fornitore Terzo, le cui presenti Condizioni Generali costituiscono parte integrante o conseguente definizione operativa relativa alle modalità di svolgimento dell'attività richiesta;

- **"Offerta di servizi"**: la scheda nella quale sono precisate le caratteristiche tecniche dei Servizi messi a disposizione dal CSI, nonché i prerequisiti che deve possedere e accettare il Fornitore Terzo per fruire degli stessi e che costituiscono allegati alle presenti Condizioni Generali;

- **"Servizio Cloud"** la disponibilità del servizio di cloud computing messo a disposizione dal CSI che permette al Fornitore Terzo di utilizzare risorse per creare una propria infrastruttura virtuale riservata e di gestire le stesse con i servizi di seguito specificati e mediante l'utilizzo di appositi software;

- **"Amministratori"**: gruppo specialistico del CSI incaricato di gestire gli apparati ed i sistemi predisposti per l'erogazione dei Servizi rivolti ai Fornitori Terzi;

- **"Nivola"**: la piattaforma cloud sviluppata dal CSI Piemonte basata sulla tecnologia open source OpenStack. La piattaforma tramite API consente di utilizzare e gestire i servizi cloud messi a disposizione dal CSI Piemonte;

- **"Service Portal"**: portale di accesso che consente tramite interfaccia web di intervenire sulle API della Piattaforma e di permettere ai Fornitori Terzi di governare i servizi Cloud necessari per l'erogazione della soluzione applicativa;

- **"POD (Point of Delivery)"** i tre ambienti fisici distinti, segregati tra loro, in luoghi differenti (entro il territorio nazionale e specificatamente nei Data Center del CSI Piemonte presso Torino e Vercelli), su cui replicare i contenuti, criteri di sicurezza e i servizi della Piattaforma Nivola;

- **"Compute Service"** il servizio IaaS erogato dal CSI attraverso la piattaforma di cloud computing Nivola basato sulle tecnologie OpenStack e VSphere; è un data center virtuale dedicato e riservato, facile e veloce da attivare, con risorse elaborative, di rete e storage configurabili e gestibili in modalità self service;

- **"Backup aaS"** è un servizio per salvaguardare le virtual machine, i dati strutturati e non strutturati all'interno della piattaforma Nivola. Non richiede infrastrutture ICT proprie perché è ospitato presso i data center del CSI-Piemonte;

- **"DBaaS"** il servizio di DataBase as a Service che permette di utilizzare un DataBase remoto ospitato nell'infrastruttura CSI; è un servizio che comprende gestione di un RDBMS e che consente ai Fornitori Terzi di ospitare dati su un Database governando solo i dati ma non il server ed i motori sottostanti;

- **"Storage aaS"** consente di associare al servizio Compute Service uno spazio disco accessibile tramite protocollo CIFS o NFS e di dividerlo tra più server virtuali.

- **"Cloud Gestito"** il servizio gestito dal CSI Piemonte per conto del Fornitore Terzo del VPC, della sicurezza dello stesso e delle virtual machine presenti;

- **"Contenuti del Fornitore"**: tutti i dati, il software, le soluzioni e le informazioni, compreso qualsiasi file, script, programma, registrazione, suono, musica, grafica, immagine, applet o servlet installato, caricato o trasferito dal Fornitore Terzo e di sua pregressa titolarità sul servizio Cloud, in quanto funzionale all'adempimento del Contratto, rispetto al trattamento di tali contenuti il CSI ai sensi dell'art. 28 del Regolamento europeo GDPR, assume il ruolo di Responsabile del Trattamento dei dati di Titolarità del Fornitore. In tale caso le modalità di svolgimento di dette attività saranno effettuate nel rispetto dei vincoli previsti nell'art. 28 sopra indicato del GDPR e delle presenti Condizioni Generali.

- **"Contenuti CSI"**: tutti i dati, il software, le soluzioni e le informazioni, compreso qualsiasi file, script, programma,

registrazione, suono, musica, grafica, immagine, applet o servlet installato, caricato o trasferito sui servizi Cloud anche a cura del Fornitore Terzo ma di titolarità del CSI e/o di un Cliente. In relazione a tali Contenuti, qualora essi contengano dati personali di un Cliente, il CSI Piemonte e il Fornitore Terzo assumono rispettivamente il ruolo di Responsabile e di sub-Responsabile del Trattamento dei dati di Titolarità del Cliente ai sensi dell'art. 28 del Regolamento europeo GDPR e come di seguito specificato; analogamente, in detta ipotesi le attività svolte dal Fornitore dovranno essere da questi effettuate nel rispetto dei vincoli contenuti nell'art. 28 del GDPR e delle presenti Condizioni Generali;

- **“Software Fornitore Terzo”**: software installato dal Fornitore Terzo in quanto detenuto in titolarità o in licenza necessario al funzionamento dei pacchetti applicativi installati dal Fornitore Terzo all'interno di Nivola;

- **“Software CSI”**: software detenuto in titolarità o in licenza del CSI Piemonte e/o di un Cliente messo a disposizione da quest'ultimo per consentire il funzionamento del servizio.

Art. 3 Modalità di attivazione dei servizi

Sottoscrivendo le presenti Condizioni Generali, il Fornitore Terzo accetta di utilizzare i Servizi Cloud di seguito descritti, o meglio contestualizzati nel Contratto, dichiarando mediante la medesima sottoscrizione di accettarne sotto la propria responsabilità relativi termini e condizioni.

Al fine di definire il dettaglio e la tipologia dei singoli servizi utili alla prestazione delle attività di cui al Contratto, sarà cura del Fornitore Terzo - previa piena comprensione ed accettazione, del perimetro, delle opzioni e dei vincoli della piattaforma cloud Nivola – indicare tramite il Service Portal le risorse e i servizi cloud di cui chiede a CSI l'attivazione. Il Fornitore Terzo prende atto di avere la possibilità di attivare e di disattivare anche solo un servizio e di aggiungere nel corso della durata del contratto, per il tramite del “Service Portal”, ulteriori servizi di interesse.

Rimane inteso che in caso di superamento del perimetro di risorse concordato tra le parti si rinvia alla disciplina del Contratto e/o alla normativa applicabile.

La fase di autenticazione per accedere al “Service Portal” non è integrata nella Piattaforma ma è gestita esternamente. Ai fini di accesso, il Fornitore Terzo dovrà utilizzare le credenziali messe previamente a disposizione dai sistemi di autenticazione del CSI. I servizi richiesti vengono attivati nel momento in cui viene perfezionato il Contratto fra le Parti e/o, in caso di non contestualità, sottoscritte le presenti Condizioni Generali. Il Fornitore Terzo riceve via email la conferma di attivazione e associazione alle credenziali fornite nella fase di perfezionamento del Contratto delle risorse richieste e il manuale d'uso.

Le credenziali così acquisite gli consentiranno di accedere al “Service Portal” con ruolo amministrativo e sarà autonomo e responsabile nel definire e gestire nel tempo le utenze e i relativi profili consentendo e revocando l'autorizzazione ad utilizzare Nivola e relativi servizi cloud secondo quanto descritto nel manuale d'uso. Solo il Referente tecnico e gli utenti con ruolo amministrativo riceveranno le segnalazioni di eventuali incidenti di sicurezza.

Nel caso in cui il Fornitore Terzo abbia difficoltà ad accedere alla piattaforma a causa di furto, smarrimento o compromissione delle credenziali, il Fornitore Terzo ha la facoltà di richiedere l'intervento telefonicamente o alla casella di posta elettronica riportata nell'art. 5.

Per tutta la durata del rapporto dovranno essere rispettate le regole di autenticazione e gestione delle credenziali, fornite in fase di attivazione del servizio stesso.

Inoltre, essendo a cura del Fornitore Terzo l'individuazione degli Incaricati Autorizzati e l'assegnazione dei ruoli, dovrà definirne un numero sufficiente per garantire una adeguata copertura per la comunicazione con CSI.

Art. 4 Caratteristiche dei Servizi

CSI mette a disposizione il Servizio senza soluzione di continuità 24 h al giorno, 7 gg la settimana, 365 gg all'anno. Per garantire tale disponibilità e l'integrità dei sistemi, il CSI adotta misure per far fronte al rischio di interruzione o altri problemi infrastrutturali, quali ad esempio la ridondanza delle infrastrutture e degli impianti, sistemi e meccanismi di alta affidabilità, sistemi di backup e di replica, canali di comunicazione sicura per i servizi che richiedono una trasmissione su rete Internet.

Qualora tra i servizi Cloud richiesti e attivati ci sia il servizio Compute Service (IaaS) può essere prevista l'attribuzione di un piano di indirizzi IP pubblici per l'accesso ad Internet, oggetto di particolari responsabilità in caso di eventuale utilizzo improprio ovvero non aderente ai contenuti degli art. 7 e 8. Tali indirizzi IP vengono riservati ed associati in fase di attivazione del servizio Compute Service e sono visualizzabili dal Service Portal. Il Fornitore Terzo potrà attestare in autonomia le soluzioni applicative e, dove concordato tra le parti, gli ambienti virtuali creati sul Compute Service sia su una rete connessa ad Internet con indirizzi IP in classe pubblica sia su una rete isolata con indirizzi IP in classe privata.

In in aderenza dell'attuale contesto normativo e delle specifiche di fornitura del Servizio, il CSI avrà cura di garantire la disponibilità dei servizi Cloud e di assicurare la qualità del Servizio offerto fino al livello dell'interfaccia web del “Service Portal”. Sarà onere del Fornitore Terzo assicurare e garantire la qualità della soluzione applicativa e/o dei beni/servizi di cui al Contratto ed acceduti dal CSI e/o dal Cliente.

Rimane inoltre inteso che il Fornitore Terzo sarà soggetto, qualora utilizzi tramite la piattaforma servizi forniti da e con altre infrastrutture, sia nazionali che estere, alle limitazioni ed alle responsabilità stabilite da ciascun gestore o operatore dei servizi stessi, conformemente con le legislazioni vigenti nei paesi ospitanti detti servizi, con le legislazioni internazionali in materia, nonché con i regolamenti di utilizzo delle infrastrutture interessate, oltre a svolgere queste operazioni attraverso gli strumenti e le funzioni offerte dal servizio cloud.

Art. 5 Assistenza Tecnica e Supporto

Il Fornitore Terzo, per la durata prevista dei servizi attivati, funzionali alle attività di cui al Contratto, potrà richiedere al CSI servizi di assistenza telematica o telefonica relativamente al funzionamento degli stessi.

Tale servizio è erogato attraverso la struttura di Assistenza che prevede:

- un forum integrato nel Service Portal contenente manuali, faq e video con le istruzioni per l'utilizzo del sistema;
- un form da compilare all'interno del Service Portal per inoltrare le proprie segnalazioni;
- una casella di posta (hd_serviziocloud@csi.it) dedicata ad accogliere le richieste di supporto;
- assistenza telefonica al numero 011/0824323.

Le ultime tre modalità sono presidiate dal lunedì al venerdì dalle ore 9 alle ore 17.

Eventuali estensioni di copertura o interventi eccezionali – nel caso funzionali agli adempimenti di cui al Contratto – potranno essere concordate tra le Parti.

In caso di interventi eccezionali o di comunicazioni riservate, sarà in ogni caso cura del CSI Piemonte contattare i referenti tecnici indicati dal Fornitore Terzo con ruolo Amministratore.

Art. 6 Garanzie e responsabilità del CSI

Nella messa a disposizione del servizio, il CSI garantisce quanto segue:

- che adotta tutte le misure tecniche, organizzative e di sicurezza atte a contrastare le minacce attualmente conosciute per proteggere adeguatamente le proprie infrastrutture e predispone le soluzioni di sicurezza perimetrale, firewall applicativi, funzionalità anti Botnet, WildFire e di intrusion detection e prevention systems;

- che il trattamento dei dati presenti nei Contenuti del Fornitore è limitato esclusivamente al fine di erogare il servizio, e non per altri scopi;

- che informerà tempestivamente il Fornitore Terzo qualora dovesse riscontrare nell'erogazione del servizio eventuali violazioni di dati personali che influiscano sui suoi Contenuti, anche al fine di consentirgli di provvedere, senza giustificato ritardo, all'eventuale notifica all'Autorità di Controllo;

- che dispone di esperti sistemisti specificatamente autorizzati alle operazioni di recupero informazioni in caso di indagini delle autorità, ma essi non svolgono in autonomia attività di indagine forense, qualificata alla investigazione e raccolta di elementi utili da essere portati in giudizio. CSI Piemonte nell'acquisizione di prove a supporto di ipotesi di commissione di reati agisce sempre su richiesta formalizzata (previo copia dell'atto di richiesta a procedere firmata dal PM) e con la supervisione dell'autorità giudiziaria. Qualora CSI Piemonte ravveda l'eventualità di una commissione di reato nelle attività di cui alle presenti Condizioni Generali, ne dà comunicazione all'autorità giudiziaria e opera su indicazione e supervisione della stessa. Nel caso i dati oggetto di richiesta dell'autorità siano trattati da CSI Piemonte in qualità di Responsabile del trattamento, salva diversa indicazione da parte dell'Autorità Giudiziaria informa il Titolare del trattamento.

- che garantisce il livello di servizio (SLA) riportato nell'offerta per ogni singolo servizio cloud necessario alla soluzione applicativa del Cliente finale.

Il CSI non effettuerà alcuna attività di sorveglianza preventiva o successiva sulla condotta degli Incaricati Autorizzati ad utilizzare i servizi Cloud per conto del Fornitore Terzo, né alcuna verifica, controllo o monitoraggio circa attività realizzati e/o gestiti dal Cliente finale tramite il Servizio.

Il CSI non verificherà, consulterà o visionerà in alcun modo i Contenuti del Fornitore Terzo, salvo nella misura richiesta dalla legge o da un organismo governativo, o da una sentenza di un tribunale competente, e/o quanto espressamente nel caso previsto dal Contratto, nei relativi ristretti limiti.

In tal caso, provvederà ad informare tempestivamente il Fornitore Terzo, fatto salvo il caso in cui il CSI è vincolato a preservare la riservatezza di un'indagine giudiziaria. Ogni attività di questo tipo sarà opportunamente registrata riportando chi vi ha acceduto, quando e quali dati sono stati divulgati.

Il CSI non si assume pertanto alcuna responsabilità per i Contenuti del Fornitore Terzo, nell'infrastruttura virtuale, attraverso gli altri Servizi erogati tramite Service Portal ed in genere per l'uso fatto dal medesimo e si riserva di adottare qualsiasi iniziativa o azione, a tutela dei propri diritti ed interessi, in caso di danni diretti o indiretti, di qualsiasi tipo e specie,

cagionato dal Fornitore Terzo ad altri soggetti che in qualsiasi modo e forma ed a qualsiasi titolo abbiano utilizzato il servizio.

Il CSI oltre agli adempimenti in materia di privacy e proprietà intellettuale, rispetta quanto previsto dalla direttiva europea NIS (UE) 2016/1148, attuata con il D.Lgs. 65/2018 per quanto riguarda la sicurezza di reti e dei sistemi informativi nell'erogazione dei propri servizi cloud. Tuttavia, tali garanzie non si estendono ai Contenuti del Fornitore e/o alle soluzioni applicative predisposte dai Fornitori Terzi.

Il CSI nel servizio offerto utilizza componenti di terze parti. Esse vengono sottoposte a rigorosi test e verifiche di sicurezza e affidabilità. Su di esse il CSI stipula accordi con i relativi fornitori e monitora le community delle componenti open source.

Il CSI si impegna, sotto la sua esclusiva responsabilità, a:

- a) garantire che la Piattaforma e tutti gli apparati a supporto (firewall, switch, router, storage ...) vengano gestiti unicamente all'interno della propria organizzazione da gruppi specialistici e debitamente formati sulle procedure di gestione, accollandosi ogni conseguente onere e responsabilità in ordine alla gestione degli accessi ai servizi e al traffico generato dalla Piattaforma;

- b) vincolare il proprio personale che opera sui servizi erogati alla riservatezza e alla non divulgazione delle informazioni a cui è venuto a conoscenza nelle attività lavorative prestata;

- c) garantire che tutti gli accessi alla Piattaforma e a tutti gli apparati a supporto da parte dei gruppi specialistici avvenga da client all'interno della propria rete privata.

- d) garantire che l'accesso da parte degli Incaricati Autorizzati e degli Amministratori avvenga solo tramite un sistema di autenticazione che richieda una password con una certa complessità, che sia cambiata regolarmente, che impedisca di riutilizzare le password più recenti, che mascheri la password sui client utilizzati per l'accesso, che la password sia cifrata durante la trasmissione e l'archiviazione, che sia impedito l'accesso tramite brute force;

- e) garantire che tutti i sistemi e gli apparati abbiano gli orari sincronizzati con un Ente esterno tramite protocollo NTP (Network Time Protocol);

- f) garantire la cifratura dei dati trasmessi su rete Internet a meno di diverse indicazioni dichiarate nella descrizione del singolo Servizio;

- g) gestire la salvaguardia dei dati (backup dei database) e delle configurazioni della Piattaforma (configurazioni dell'infrastruttura) e il loro eventuale ripristino per garantire le condizioni di servizio concordate. Tutte le attività inerenti il servizio (accesso, ripristino, applicazione delle policy), il nome dell'Amministratore e i dati interessati (ad esempio i database) saranno registrati dagli strumenti di salvaguardia adottati da CSI e resi disponibili al Fornitore Terzo, per le parti di sua competenza, su richiesta e con tempi e modi da definire in funzione dell'ampiezza del volume interessato; inoltre per il servizio di Backup aaS è previsto che il CSI si occuperà sia della salvaguardia delle virtual machine secondo le politiche di ritenzione concordate con il Cliente che del ripristino su richiesta del Fornitore Terzo e questi dati saranno presenti solo nella sede presso la quale si è deciso di attivare il servizio;

- h) securizzare gli ambienti gestiti dal CSI necessari a garantire il corretto funzionamento della Piattaforma e dei servizi che la compongono, impegnandosi a sua cura e spesa nell'adozione di anti-malware e anti-virus;

- i) aggiornare le componenti hardware e software della Piattaforma o predisporre di nuovi, seguendo un processo che prevede sia rigorosi test che il collaudo propedeutici al rilascio per mitigare/eliminare malfunzionamenti con particolare attenzione alla protezione dei dati, la valutazione e correzione delle vulnerabilità, eliminazione di back doors, modifiche non

autorizzate, integrità delle configurazioni, registrare i cambiamenti ed eventualmente ripristinare la versione precedente;

j) predisporre ambienti distinti, segregati e securizzati per lo sviluppo e il test a supporto del processo di rilascio e di aggiornamento, coinvolgendo sistemi, apparati e dati propri, distinti dall'ambiente produttivo dove non sono presenti i codici sorgenti che sono archiviati su repository ad hoc;

k) gestire e custodire secondo i termini di legge il registro degli eventi generati dalla Piattaforma e dai servizi gestiti (Backup, DB, Storage as a service). Tali informazioni potranno essere messe a disposizione del Fornitore Terzo, con tempi e modi da definire in funzione dell'ampiezza del volume interessato, e/o all'autorità giudiziaria (es. Polizia Postale, Garante o Forze dell'Ordine) per ottemperare a richieste giudiziarie o amministrative qualora esplicitamente da questi richiesto come previsto dalla normativa vigente; Sono esclusi i log degli ambiti riportati nel punto i) art. 7 Obblighi e Responsabilità del Fornitore Terzo e punto d) art.8 Obblighi e Responsabilità del Fornitore Terzo in assenza di "Cloud Gestito";

l) avviare con cadenza almeno semestrale attività di analisi di sicurezza per rilevare eventuali criticità ed apportare eventuali modifiche alla Piattaforma in modo conforme al processo di aggiornamento e di rilascio;

m) monitorare i sistemi e le componenti applicative della Piattaforma Nivola al fine di intervenire tempestivamente in caso di malfunzionamenti o carenze di risorse;

n) assicurare che lo spazio disco messo a disposizione dei Fornitori Terzi non contenga dati visibili legati a servizi precedenti;

o) monitorare il traffico di rete verso i propri apparati, diretti ai sistemi virtuali dei Fornitori Terzi. In caso di attività anomala, che potrebbero rivelarsi attacchi informatici, il CSI provvederà all'inibizione del traffico verso i sistemi virtuali oggetto del presunto attacco ed informerà subito dopo il Fornitore Terzo (ovvero l'incaricato autorizzato in fase di attivazione o altro delegato) nonché ove del caso il Cliente dell'accaduto seguendo le modalità offerte dalla Piattaforma ed eventualmente anche le autorità competenti;

p) mantenere i contatti con gruppi e persone specializzate sulla sicurezza informatica in modo da garantire una continua azione di miglioramento;

q) replicare i contenuti, criteri di sicurezza e i servizi della Piattaforma Nivola su tre ambienti fisici distinti chiamati POD (Point of Delivery), segregati tra loro, in luoghi differenti (entro il territorio nazionale) e di mettere a disposizione dei Fornitori Terzi opportuni strumenti per predisporre in autonomia i propri processi di Business Continuity, ove funzionali alle attività di cui al Contratto. Lo stato delle repliche è verificato con gli strumenti di controllo della piattaforma;

r) prevedere un RPO ed un RTO di 24 h per tutti i dati del Fornitore Terzo;

s) cancellare i dati temporanei prodotti in attività di aggiornamento hardware e/o software dalla Piattaforma;

t) condividere con i Clienti e Fornitori Terzi attraverso la Piattaforma Nivola o altri strumenti di comunicazione eventuali minacce a livello di sicurezza informatica e di come sono gestite;

u) collabora con i Fornitori Terzi per assicurare la correzione/cancellazione dei dati che il Titolare del trattamento richiede in conseguenza degli obblighi derivanti dalle norme Privacy (per esempio cancellazione dei salvataggi);

v) Fornire sul Service Portal l'elenco dei fornitori relativi alla Piattaforma Nivola qualora possano accedere a dati personali.

w) Richiedere, secondo le modalità offerte dalla Piattaforma, esplicita autorizzazione del Cliente e del Fornitore del Servizio

qualora fosse necessario accedere ai dati dello stesso da parte CSI per poter effettuare analisi di problem determination;

x) analizzare sistematicamente i propri i propri log di accesso al portale ed i log dei task ed operazioni effettuati sulla piattaforma cloud al fine di rilevare eventuali tentativi di accessi non autorizzati o attacchi;

y) in caso di violazione di dati personali residenti su apparati e sistemi gestiti da CSI, saranno informati entro 48 ore il Titolare del trattamento dei Dati, descrivendo l'accaduto (specificando se si tratta di perdita, divulgazione o alterazione delle informazioni), fornendo il supporto necessario secondo le indicazioni del Titolare allo scopo di individuare le conseguenze e le azioni per il ripristino, ottemperando a quanto previsto nel GDPR nei casi di data breach.

Art. 7 Obblighi e responsabilità del Fornitore Terzo

Il Fornitore Terzo è l'unico ed esclusivo responsabile di tutte le attività eventualmente svolte dai suoi Incaricati Autorizzati che sono pertanto sotto il suo esclusivo controllo, nonché di tutti i Contenuti – sia propri sia realizzati eventualmente in ragione del Contratto - discrezionalmente realizzati e/o memorizzati tramite il Servizio, ed eventualmente condivisi con terze parti, con il CSI e/o con il Cliente.

Il Fornitore Terzo è anche responsabile, e se ne assume i relativi costi di supporti o manutenzioni, delle licenze software eventualmente necessarie al funzionamento dei pacchetti applicativi da lui installati ed utilizzati, inclusa la loro fruibilità nei termini e modi funzionali alle attività di cui al Contratto.

Il CSI si limiterà pertanto a mettere a disposizione le capacità elaborative, i servizi e gli strumenti, come richiesti dal Fornitore Terzo ai sensi dell'art. 3, senza esercitare alcun tipo di sorveglianza sulle attività svolte e/o sui Contenuti ivi salvati dagli Incaricati Autorizzati e senza svolgere alcun controllo o verifica sulla correttezza o sulla liceità delle licenze. I servizi saranno erogati nella modalità "Cloud Gestito" o "Gestione del S.O.", nei quali il CSI si farà carico delle attività di gestione delle infrastrutture con un diverso perimetro definito. Rimangono a carico completo del Fornitore Terzo costi di acquisto, supporto o manutenzione, delle licenze software eventualmente necessarie al funzionamento dei pacchetti applicativi da lui installati ed utilizzati.

Sottoscrivendo le presenti Condizioni, il Fornitore Terzo si impegna, sotto la sua esclusiva responsabilità, a:

a) garantire che il Servizio venga utilizzato unicamente ai fini di cui al Contratto, da parte di incaricati autorizzati, accollandosi ogni conseguente onere e responsabilità in ordine alla gestione degli accessi ai servizi e al traffico generato ed immesso sulla Piattaforma; nel caso di adesione al servizio "Cloud Gestito", il CSI Piemonte si occuperà della gestione degli accessi al VPC, mentre nel caso di adesione al servizio "Gestione del S.O.", il CSI Piemonte si occuperà della gestione degli accessi al sistema operativo delle singole virtual machine, ivi comprese la registrazione e conservazione degli accessi a norma di legge;

b) fatte salve le eventuali previsioni di cui al Contratto in termini di Subappalto, che dovranno comunque essere debitamente formalizzate, non cedere a terzi in tutto o in parte l'uso del Servizio, senza il preventivo consenso scritto del CSI e non divulgare, direttamente o indirettamente anche tramite il proprio personale, password e/o login e/o comunque chiavi di accesso; c) utilizzare i Servizi richiesti esclusivamente per i fini di cui al Contratto, ed in ogni caso per scopi leciti e ammessi dalle disposizioni di legge, dagli usi e consuetudini, dalle regole di diligenza, senza ledere qualsivoglia diritto di terzi e in ogni caso, garantire il rispetto, anche da parte dei propri Incaricati

Autorizzati, della vigente normativa, comprese le leggi sulla privacy e sul copyright e le norme delle presenti Condizioni Generali;

d) non installare software tale da poter compromettere il buon funzionamento dei propri ambienti e della Piattaforma Nivola;

e) informare tempestivamente il CSI di qualsiasi uso non autorizzato del proprio Servizio o di qualsiasi altra violazione della sicurezza riscontrata;

f) collaborare con il CSI nelle attività eventualmente richieste dal Cliente Titolare del trattamento dati in conseguenza degli obblighi derivanti dalla normativa applicabile in tema di protezione dei dati personali;

g) riconoscere e prendere atto che il trattamento di dati e/o informazioni e/o contenuti attraverso la piattaforma del CSI e la conseguente loro diffusione nella rete Internet attraverso la medesima infrastruttura deve essere eseguito in osservanza dei principi fondamentali della legislazione europea in materia di protezione dei dati personali. In particolare deve essere garantita la trasparenza nei confronti degli interessati coinvolti nel trattamento dei dati personali di titolarità del Cliente, deve essere rispettato il principio della specificazione e limitazione delle finalità e i dati personali devono essere cancellati non appena la loro conservazione nell'infrastruttura del CSI non è più necessaria. In quest'ultimo caso CSI e Fornitore Terzo devono sostenere il Cliente, Titolare del trattamento, nell'agevolare l'esercizio dei diritti degli interessati di accedere ai loro dati, nonché rettificarli o cancellarli e garantire che la cancellazione dei contenuti compiuta dal Fornitore Terzo è effettuata in modo sicuro e irrecuperabile e che non viene conservata alcuna copia;

h) gestire e custodire secondo i termini legislativi il registro degli eventi generati dalle soluzioni applicative e da tutti gli strumenti predisposti dal Fornitore Terzo (si intendano ad esempio i log della soluzione applicativa);

i) richiedere l'attivazione del servizio di salvaguardia dei dati e il loro ripristino, attraverso gli strumenti e le regole di ritenzione previsti e proposti dal CSI.

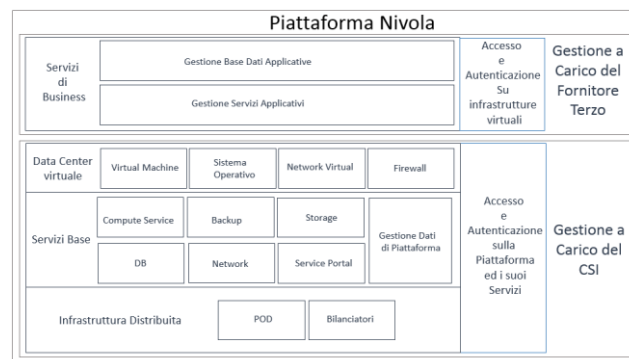
l) manlevare e tenere indenne il CSI da ogni e qualsiasi domanda o pretesa di risarcimento danni, diretta o indiretta, di qualsiasi natura e specie, comprese le eventuali spese legali, da chiunque avanzata al riguardo e derivanti dall'utilizzo improprio sia del servizio cloud che delle soluzioni applicative da parte di soggetti comunque ingaggiati nell'interesse del Fornitore Terzo,

m) predisporre in autonomia i propri processi di Continuità Operativa, selezionare i propri servizi applicativi coinvolti e predisporre le policy di utilizzo, avvalendosi degli strumenti messi a disposizione del CSI e con propri compatibili con la piattaforma.

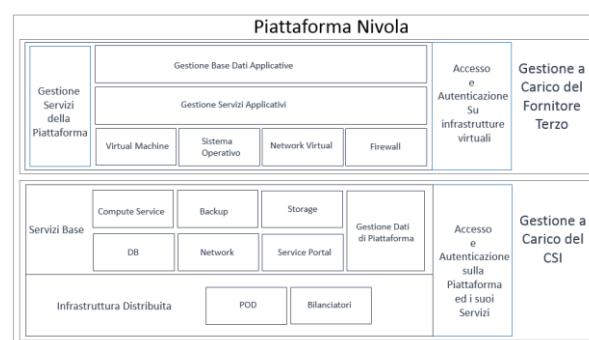
n) garantire che le soluzioni applicative ospitate con gli strumenti messi a disposizione della Piattaforma, garantiscano livelli di servizio (SLA) compatibili con quelli offerti dal CSI, che, in caso contrario, non sarà in alcun modo responsabile;

L'immagine sottostante riassume e descrive graficamente le competenze e le responsabilità del Fornitore Terzo e del CSI Piemonte,

a) nel caso di "cloud Gestito":



b) in assenza di "Cloud gestito":



Art. 8 Ulteriori obblighi e responsabilità del Fornitore Terzo in assenza di "Cloud Gestito"

Il Fornitore Terzo che non si avvale della modalità "Cloud Gestito" oltre ad assumere gli obblighi e responsabilità previste all'art. 7 dovrà seguire le indicazioni riportate nel seguente articolo.

Acconsentendo l'attivazione dei Servizi e sottoscrivendo le presenti Condizioni, il Fornitore Terzo si impegna, sotto la sua esclusiva responsabilità, a:

a) securizzare gli ambienti virtuali creati sul compute Service, cambiare al primo avvio la password di default dell'utenza amministrativa presente sugli ambienti disponibili a catalogo (root su sistemi operativi Linux, administrator su sistemi operativi Microsoft Windows) e in ogni caso compiere ogni altra attività ritenuta utile o necessaria a garantirne la sicurezza e l'integrità impegnandosi a sua cura e spese, nell'adozione di misure di sicurezza idonee ed adeguate a protezione dei dati (quali per esempio l'installazione di anti-malware e anti-virus);

b) farsi autonomamente carico di acquisire l'insieme delle conoscenze tecniche necessarie ad assicurare la corretta utilizzazione, amministrazione e gestione dei Servizi Cloud e del servizio di business.

c) gestire e custodire secondo i termini legislativi il registro degli eventi generati dai sistemi virtuali e dai servizi controllati direttamente (si intendano ad esempio i log dei sistemi operativi virtuali);

d) prevedere regole, procedure e strumenti per la cifratura delle informazioni e dei dati trasmessi e conservati dal servizio di business, a meno che non siano già previsti esplicitamente nella descrizione dei servizi offerti da CSI;

e) monitorare attraverso gli strumenti messi a disposizione le risorse assegnate sulla Piattaforma Nivola al fine di rilevare

tempestivamente carenze di risorse ed intervenire riorganizzandole o richiedendone di ulteriori.

Art. 9 Interruzione del Servizio

Il CSI si riserva la facoltà di interrompere la fornitura del Servizio, concordandone con il Cliente ed il Fornitore tempistiche e modalità, per procedere ad interventi tecnici finalizzati a migliorarne il funzionamento o dandone comunque tempestiva comunicazione al Cliente e al Fornitore Terzo qualora vi siano fondati motivi per ritenere che ci possano essere problemi di sicurezza e/o di tutela del diritto di riservatezza ovvero nei casi di forza maggiore.

Rimane inteso che in tale ipotesi sarà cura di tutte le parti coinvolte definire le migliori modalità per non arrecare interruzioni e/o problematiche relative alle attività di cui al Contratto.

Art. 10 Cessazione o dismissione del servizio

In caso di cessazione per qualunque causa del rapporto di cui al Contratto, e/op eventuale ridefinizione degli accordi ivi previsti che comunque implichino la cessazione del servizio di cui alle presenti Condizioni Generali, rimane inteso ed accettato che:

- il CSI disporrà dei dati afferenti al Fornitore Terzo, nonché dei Contenuti del Fornitore, secondo le direttive che il Fornitore Terzo stesso avrà indicato. Ove il Fornitore Terzo non abbia comunicato dette direttive entro e non oltre 15 giorni a decorrere dalla data di avvenuta cessazione del rapporto per qualunque causa, il CSI non avrà alcun onere e impegno connesso e/o derivante dalla gestione dei dati del Fornitore Terzo e, trascorsi ulteriori 30 gg, provvederà alla cancellazione e rimozione dei suoi Contenuti.

- il Fornitore dovrà invece consegnare in forma intellegibile, in formato aperto e compatibile con la Piattaforma i Contenuti del CSI/del Cliente trattati e/o creati in corso di attività di cui al Contratto, senza conservarne copia in qualsivoglia forma;

Tutti i contenuti del Fornitore non funzionali alla fruizione dei Contenuti del CSI/Cliente saranno comunque cancellati in modalità “sicura” e irreversibile e saranno distrutti trascorsi 45

gg dal momento della comunicazione della dismissione del servizio, senza possibilità di recupero. Sarà cura del CSI fornire tramite mail al Fornitore Terzo, con ruolo amministratore, un report contenente tutti i comandi e l'esito della cancellazione dei dati interessati, e che in nessun caso sono coinvolti supporti removibili per memorizzare il dato. Di conseguenza, il Fornitore Terzo dovrà a sua esclusiva cura effettuare il salvataggio dei contenuti inseriti e gestiti tramite il servizio, prima della data della dismissione. Questo trattamento sarà riservato a tutti i dati del Fornitore Terzo residenti su tutti gli ambienti distinti (incluso il backup), segregati e replicati della Piattaforma Nivola.

Art. 11 Modifica delle condizioni

In qualsiasi momento il CSI si riserva la possibilità di modificare o integrare le presenti Condizioni. Di tale modifica sarà data opportuna conoscenza mediante pubblicazione su “Service Portal” e invio delle suddette modifiche e/o integrazioni agli indirizzi e-mail dei Fornitori Terzi indicati come Referenti tecnici.

Trascorsi trenta giorni dalla ricezione, qualunque modifica o integrazione alle presenti Condizioni Generali saranno considerate accettate.

Le presenti Condizioni Generali costituisce manifestazione univoca ed integrale dei rapporti che intercorrono tra il CSI ed il Fornitore Terzo con riferimento ai servizi Cloud superando ed annullando ogni diversa precedente intesa relativamente al Servizio oggetto dello stesso.

Firma: _____

Timbro: