AUP - Acceptable Use Policy Servizio Cloud

Premessa

La presente pagina stabilisce le regole base e le responsabilità del Cliente riguardanti il corretto utilizzo del servizio. La violazione di queste Policy può tradursi in una immediata sospensione o terminazione del servizio, in accordo con le condizioni di fornitura inserite nel contratto.

Eventuali chiarimenti riguardanti questo documento devono essere richiesti al proprio Demand Manager (la figura che ha seguito il committente nella formalizzazione del contratto analizzandone i requisiti).

Incidenti e violazioni

E' vietato utilizzare la rete o le risorse Cineca per promuovere o condurre attività illecite, o comportamenti irresponsabili che includano ad esempio:

- utilizzare la rete o i servizi per offrire sistemi di anonimizzazione, a meno di mantenere un'adeguata tracciabilità delle identità come prescrive la legislazione, in caso di richieste delle autorità giudiziarie;
- usare il servizio per distribuire o utilizzare software che raccoglie informazioni sull'utilizzatore generico e li trasmette senza il suo consenso o consapevolezza (tutela della privacy a carico del cliente);
- uso non autorizzato o accessi non autorizzati a sistemi e reti terze (scansioni o tentativi di analisi delle vulnerabilità perpretrati verso target esterni o interni l'infrastruttura Cineca);
- effettuare attività che interferiscono con l'utilizzo del servizio da parte di ogni utente, causando disservizi o danni diretti, inclusi tentativi di brute force, diffusione di malware, attacchi informatici inclusi DOS o DDoS che provochino saturazione di risorse, inclusa la rete;
- utilizzare software piratato, crackato o eludere il pagamento delle licenze dei fornitori;
- violare copyright anche in termini di distribuzione di contenuti coperti da tale vincolo;
- raccogliere o usare contatti di posta elettronica, nomi o altri ID senza il consenso dell'interessato (spam, phishing, furti di identità, ecc.);
- utilizzare distribuzioni di servizi software noti come ADware a meno che non si possegga il permesso dell'utente di scaricare il software, che il software sia removibile facilmente e con il solo uso di comandi e funzioni del sistema operativo come ad esempio Add/Remove programs di Windows;
- istallare applicazioni che possono causare interruzioni di servizio o di infrastruttura a Cineca o terzi;
- offrire servizi di open relay o open proxy;
- offrire informazioni pubbliche, in qualunque forma, che siano a danno del servizio Cloud fornito da Cineca.

Email di SPAM

E' vietato diffondere messaggi per campagne mail (es.marketing) a meno che:

- esista il consenso del destinatario all'invio di tali messaggi
- sia visibile in modo chiaro per il ricevente l'istruzione per evitare di ricevere ulteriori messaggi e che le richieste di rimozione effettuate siano prontamente soddisfatte (entro 48h dalla richiesta dell'interessato);
- le procedure per registrare il consenso del destinatario ne verifichino l'effettiva identità;
- si abbia la possibilità di produrre la prova dell'avvenuto consenso entro 72 ore dalla richiesta di Cineca;

Non è inoltre ammesso che venga mascherato l'indirizzo del mittente, che deve pertanto apparire nel corpo o nel From del messaggio. Tali regole si applicano anche a servizi software automatici e riguarda anche recipients eventualmente presenti in sistemi ospitati dal servizio Cloud. Lo stesso dicasi per servizi email di terze parti, se questi non applicano quanto sopra descritto. Resta inteso che Cineca può filtrare la trasmissione di mail se questi requisiti non venissero rispettati.

Test di Vulnerabilità

I clienti non potranno in nessun modo fare scansioni, tentativi di penetrazione o test di vulnerabilità dei sistemi di gestione e di autenticazione di Cineca o sulla infrastruttura Cloud condivisa. Non potranno effettuare tali test (eseguiti in proprio o tramite terze parti) neanche sul proprio Tenanat, sia usando tecniche passive sia attive ed invasive, a meno di aver chiesto espresso consenso scritto di Cineca. Attività di questo tipo verranno recepite come attacchi infrastrutturali e potrebbero scatenare azioni di trattamento degli incidenti o reattive, con conseguenze anche di tipo legale. Per effettuare tali attività sulla propria infrastruttura è necessario chiedere e attendere autorizzazione a Cineca per tramite del servizio di supporto (custometportal.cineca.it) specificando almeno (si veda in dettaglio la pagina Regolamentazione attività di VAPT):

  - Motivazione della richiesta
  - Durata e slot temporali
  - Tipologia di attività
  - Range di IP sorgente/destinazione coinvolti
  - occupazione di banda prevista.

Cineca si riserva il diritto di richiedere lo stop dell'azione di VAPT al manifestarsi di problemi sul carico dei sistemi che danneggino le performance di altri tenant.

Cineca da parte sua effettua periodicamente test di vulnerabilità sull'infrastruttura e gli strumenti di gestione della stessa come prescritto dalle norme ISO 27001 cui è conforme e certificato, vedi https://www.cineca.it/it/content/certificazioni.

Uso delle risorse

L'utente cloud non deve usare il servizio in modo improprio, ad esempio sottoponendo le infrastrutture a test di carico tramite software, anche agendo al di fuori del perimetro del Cloud stesso, esaurendo la capacità della rete, del sistema di storage, della CPU o di ogni altra risorsa messa a disposizione, essendo in un contesto di infrastruttura condivisa. Questo modo di agire infatti potrebbe causare danni ad altri utilizzatori della stessa infrastruttura. In tal caso Cineca può chiedere l'immediato ripristino delle condizioni normali, per evitare il conflitto di risorse di altri clienti.

Contenuto offensivo

Il cliente non deve trasmettere, memorizzare, postare o rendere pubblico tramite la rete di Cineca contenuti che:

- promuovono o hanno a che fare in qualunque modo con: pedofilia, odio razziale o analoghi casi esclusi dalla legislazione vigente;
- incitino alla violenza, all'aggressione, siano minacciosi o espressione di odio;
- contenuti diffamatori o in violazione alla privacy di una o più persone;
- creino un rischio per la salute, la sicurezza e i diritti delle persone o per la sicurezza nazionale;
- violino copyright, brevetti, marchi o altri diritti proprietari;
- promuovano il gioco d'azzardo illegale, droghe, o altre attività illecite;
- siano maliziosi, fraudolenti o passibili di produrre azioni legali ai danni di Cineca.

Tali attività non possono essere effettuate con qualunque sistema (web, mail, chat o altro), se appartenente alla rete Cineca con cui il servizio viene erogato.

Contenuti o articoli soggetti a diritti di autore

E' vietato utilizzare la rete Cineca per scaricare, pubblicare, distribuire, copiare o utilizzare qualunque testo, musica, software, prodotto artistico, immagine o altri articoli protetti da copyright, brevetti, protezione di marchi a meno di poter esibilre l'autorizzazione dell'autore stesso.

Blacklist o uso corretto della rete

Il Cliente accetta inoltre che qualora i propri indirizzi IP pubblici siano stati inseriti in una blacklist di anti spam (es. spamhouse.org) Cineca potrebbe imputare al Cliente la violazione della presente AUP, adottando tutti i provvedimenti ritenuti idonei a proteggere i propri IP, tra cui l'eventuale sospensione o cessazione del servizio, indipendentemente dal fatto che l'iscrizione nella blacklist sia riconducibile al Cliente o conseguenza di una violazione di terzi sulle proprie macchine.

Il Cliente si impegna inoltre ad osservare le norme di comportamento nell'uso della rete Internet comunemente definite come "Netiquette" https://it.wikipedia.org/wiki/Netiquette.

SLA e penali

Non è prevista nessuna penale derivante dal superamento delle soglie di SLA per interruzioni che derivino da violazioni della presente AUP.

GDPR - trattamento di dati personali o particolari

Il COMMITTENTE è tenuto a rispettare i requisiti del Regolamento Europeo 2016/679/EU (GDPR) in termini di protezione dei dati personali o particolari che possono essere oggetto di trattamento presso i sistemi ospitati in Cineca, con totale responsabilità nei casi dei servizi IAAS e PAAS, rispetto ai quali Cineca non esercita alcun tipo di attività di trattamento se non di tipo tecnico e indiretto e di cui non è a conoscenza, fatta eccezione per il backup automatizzato di macchine virtuali del Cliente.

Saranno comunicati dal Committente i recapiti delle figure incaricate a gestire problematiche inerenti il trattamento dei dati (ad es. il DPO e coloro che possono autorizzare richieste di accesso, estrazioni, etc). Dal canto suo il provider garantisce il rispetto della segregazione dei compiti, la gestione secondo la normativa vigente delle autorizzazioni agli Amministratori di Sistema ed al logging dei loro accessi, la gestione corretta dei sub-fornitori, l'assistenza al Titolare rispetto all'adempimento di quanto utile o necessario a garantire la sicurezza dei dati e al trattamento di eventuali Data Breach e ogni altra misura di sicurezza adeguata all'incarico ricevuto.

Il contatto in caso di problematiche relative a questo paragrafo è disponibile all'indirizzo mail, alla quale risponde il DPO Cineca: privacy_at_cineca.it

Segnalazioni di Data Breach (violazioni di dati personali) per i quali Cineca abbia una parte attiva come responsabile del trattamento o come titolare, è possibile inoltrarle tramite la coda SD DATABReach visibile sempre tramite Customerportal, nell' area "Servizi Infrastrutturali"